My First Bitcoin
EL SALVADOR

Bitcoin Diploma

Financial Education for the Bitcoin Era

Student Workbook

English Version | 2025

Bitcoin Diploma

Financial Education for the Bitcoin Era

Student Workbook

English Version | 2025

My First Bitcoin

EL SALVADOR

DONATE NOW

bc1q5es60qpa7gpkp0k32xl4zefkj43kd9zjkzd54sgmv3yzr34dw8dqm9pzsd

The Bitcoin Diploma Story

There is nothing more powerful than an idea whose time has come.

The Bitcoin Diploma story began in El Salvador, with the first pilot of 38 public school students graduating in June 2022—this was the first Bitcoin Diploma in a public school system anywhere in the world.

It's hard to believe that was less than three years ago.

The growth since then has been phenomenal, with thousands of Bitcoin Diploma graduates from our classes all over the nation. However, the most exciting and inspiring growth has come from others. The workbook is open-source, and an incredibly diverse collection of Bitcoin educators have embraced the material, both in El Salvador and beyond.

The Ministry of Education in El Salvador used it as the primary source material for its own Bitcoin Diploma, and in 2024, we joined with Bitcoin Beach to train over 400 public school teachers to teach it in their schools.

One of our original goals was to teach a nation and demonstrate Bitcoin education as a force for good at mass scale. That dream is now well on its way.

El Salvador is the focus; the mission is the world.

In March 2023, we founded the international Bitcoin Educators Node Network, requiring all nodes to agree to some core principles: that the education must be independent, impartial, community-led, bitcoin-only, high quality, and empowerment-focused. This network, now self-governing, has translated the work into more than eight languages and taught the Bitcoin Diploma in Canada, the US, Mexico, Guatemala, Honduras, Costa Rica, Cuba, the Dominican Republic, Haiti, Colombia, Suriname, Peru, Brazil, Argentina, Ireland, the UK, Portugal, Georgia, Ghana, Nigeria, Uganda, Kenya, Zambia, Zimbabwe, South Africa, Afghanistan, Bangladesh, India, Hong Kong, Indonesia, and Australia. The network adds new nodes each month, and since the work is open-source, no one needs permission. Many more have likely done this completely on their own.

This is a global, decentralized movement.

Independent, impartial, community-led Bitcoin education will change the world. It already has.

For a better world,

My First Bitcoin team, 2025

Table of Contents

Chapter #1: Why Do We Need Money?

1.0 Introduction 01

1.1 Meet Satoshi 01

Activity: Five Questions on Money 01

1.2 Class Discussion — Why Do We Need Money? 04

Chapter #2: What Is Money?

2.0 Introduction 07

Activity: Class Discussion - "What is Money?" 07

2.1 Definition of Money 07

2.2 Function of Money 09

2.3 Properties of Money 10

2.4 Types of Money 13

2.5 The Psychology of Money: Scarcity, Time Preference, and Trade-Offs 14

Activity: Time Preference 16

Chapter #3: The History of Money

3.0 Introduction 21

Activity: Barter Game 21

3.1 Evolution from Barter to Modern Currency 23

3.1.1 Problems with Early Forms of Money 23

3.1.2 Development of Coinage and Paper Money 24

3.1.3 Transition from Sound to Unsound Money 25

3.1.4 Paper to Plastic 27

3.2 Digital Currency 28

Chapter #4: What Is Fiat Money and Who Controls It?

4.0 Introduction 31

4.1 Brief History of Fiat Money 31

4.2 The Fiat System 34

4.2.1 A Monetary System by Decree 34

4.2.2 Fractional Reserve Banking: A System Fueled by Debt 35
Activity: Fractional Reserve Banking 38
4.2.3 Who Controls the Fiat System and How Do They Benefit? 39
4.3 Central Bank Digital Currencies: The Future of Fiat Money 41

Chapter #5: How Problems Lead to Solutions

5.0 Introduction to the Problem 45
5.1 Decreasing Purchasing Power 45
5.1.1 Monetary Inflation and Its Effect on Purchasing Power 45
Activity: The Effects of Inflation — An Auction Activity 46
5.2 The Global Debt Burden and Social Inequality 47
5.2.1 Impact on the individual — Loss of Purchasing Power 47
5.2.2 Impact on Society — Increasing Wealth Inequality 52
Activity: Consequences of the Fiat System 53
5.2.3 The Global Debt Burden 54
5.3 The Cypherpunks and the Quest for a Decentralized Currency 55
5.3.1 The Cypherpunks 56
5.3.2 Centralized vs. Decentralized Systems 57
5.3.3 Brief History of Digital Currencies 59

Chapter #6: An Introduction to Bitcoin

6.0 Satoshi Nakamoto and the Creation of Bitcoin 63
6.1 How Does Bitcoin Work? 65
6.1.1 The Nakamoto Consensus Mechanism 65
6.1.2 The Players of the Game 67
Activity: Consensus Building in a Peer-to-Peer Network 69
6.2 Bitcoin as Sound Digital Money 71
6.2.1 Introduction 71
6.2.2 Bitcoin's Features 72
Activity: Class Discussion — Is Bitcoin Sound Money? 76
6.2.3 Embracing Personal Responsibility 76

Chapter #7: How to Use Bitcoin

7.0 Introduction 81

7.1 Acquiring and Exchanging Bitcoin 81

7.1.1 P2P: Physical 81

7.1.2 P2P: Online 82

7.1.3 Centralized Exchanges 82

7.2 An Introduction to Bitcoin Wallets 83

7.2.1 Self-Custodial vs Custodial Wallets 83

7.2.2 Different Types of Bitcoin Wallets 85

7.3.3 Open Source vs Closed Source 86

Activity: Class Evaluation of Bitcoin Wallets 87

7.3 Setting Up a Mobile Bitcoin Wallet 87

Activity: Setting Up/Recovering a Bitcoin Wallet 87

7.4 Receiving and Sending Transactions 89

Activity: Bitcoin Transactions in Action 91

7.5 Saving in Bitcoin 93

7.6 Don't Trust, Verify 94

Chapter #8: Lightning Network: Using bitcoin in your daily life

8.0 Introduction 97

Activity: Watch "Bitcoin Lightning Network Explained: How it Actually Works" 98

8.1 The Lightning Network 98

8.2 Different Types of Lightning Wallets 100

8.2.1 Self-Custodial vs. Custodial Wallets 100

8.2.2 Open Source vs. Closed Source 100

8.3 Setting Up a Bitcoin Lightning Wallet 100

8.4 Sending and Receiving Lightning Transactions 102

Activity: Lightning Wallet Relay Race 106

8.5 Buying Coffee and Groceries with Bitcoin 107

8.5.1 Online: Payment Plugins — Ecommerce 108

8.5.2 In Person: Find a Merchant in Your Area 109

8.5.3 Transitional Tools: Gift Cards and Payment Cards 110

8.5.4 Circular Economies and Bitcoin as a Medium of Exchange 110

Chapter #9: An Introduction to the Technical Side of Bitcoin

9.0 Introduction 115

Activity: Watch "How Bitcoin Works under the Hood" 115

9.1 Public and Private Keys: Security through Cryptography 116

9.1.1 Cryptography Public/Private Keys 116

9.1.2 Hashing Explanation 119

Activity: Generate SHA 256 Hash 121

9.2 The UTXO Model 122

9.3 A Closer Look at Bitcoin Nodes and Miners 125

9.3.1 What Is a Bitcoin Node and How Do I Set One Up? 125

Activity: Watch Video on Bitcoin Nodes 126

9.3.2 What Is a Bitcoin Miner and How Does Mining Work? 126

9.4 What Is the Mempool? 132

Activity: Mempool 134

9.5 How Bitcoin Transactions Work from Start to Finish 135

Chapter #10: Why Bitcoin?

10.0 Introduction 139

Activity: What Could a Bitcoin Future Look Like? 139

10.1 What Are Central Bank Digital Currencies (CBDCs) and Who Controls Them? 140

10.2 The Philosophy of Bitcoin 141

Activity: Class Discussion — Do You Have the Right to Control Your Own Money? 141

10.3 The Benefits of Bitcoin 142

10.4 An Empowered Future 143

Activity: Class Discussion — How Did Your Perspective Change? 143

Additional Resources 147

Chapter Key Concepts 149

Glossary 153

Bitcoin Diploma

A 10-Week Transformational Journey
through Independent, Impartial,
High-Quality, and Free Education

It is essential to have a firm grasp of the basics of money, its history, and the current financial system before studying Bitcoin. Understanding these concepts provides a strong foundation for comprehending Bitcoin's unique and disruptive nature. By learning about the evolution of money, you will be able to better understand the potential and limitations of the current financial system and how Bitcoin aims to address them. Without this foundation, it may be challenging to fully appreciate Bitcoin's significance and potential impact. Trust the process of learning and stay focused, as the reward of a deeper understanding and appreciation of this cutting-edge field will be well worth it.

Chapter #1

Why Do We Need Money?

1.0 Introduction

1.1 Meet Satoshi

Activity: Five Questions on Money

1.2 Class Discussion — Why Do We Need Money?

Student Workbook

English Version | 2025

Why Do We Need Money?

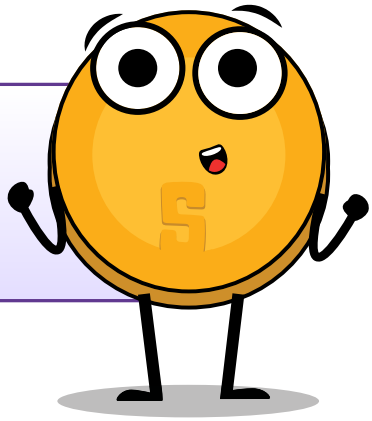
1.0 Introduction

> Money is one of the greatest instruments of freedom ever invented by man.
>
> **Friedrich Hayek**

Welcome to the Bitcoin Diploma. In this chapter, we'll explore the fundamental question of why money is essential in our lives. We'll look into the nature of money and its various forms, aiming to gain a deeper understanding of its significance. Money is something we use almost every day, but do we actually understand why we need it and what it is? Why do our parents and other family members trade their time for money? Why do some people have more of it than others? Why is money different in other countries? Why can't we just create more of it when we need it?

1.1 Meet Satoshi

> ***Hi! I'm Satoshi, an interactive assistant who will help you throughout the Bitcoin Diploma. I will give you resources and helpful recommendations so you can take a closer look at key concepts.***



Activity: Let's Start the Chapter by Answering the Five Questions Below:

Consider practical uses like acquiring necessities such as food and desired items. Try to be specific in your examples, balancing creativity with realism.

Why do we need money?

What is money?

Why Do We Need Money?

Who controls money?

What gives money its "value"?

What question do you have about money? Write down your question here to share with the class.

Expand the discussion to the whole class, sharing and comparing lists to determine the five most essential reasons for needing money. Identify common ideas across the class. Reflect on your individual unique ideas that didn't make the list but are worth considering. Jot down these additional insights.

1.2 Class Discussion — Why Do We Need Money?

The Class will split into groups and:

- Share and discuss their answers to the first four questions. Write down their favorite answers.
- Share their answers to the last question and vote for one favorite student-question. Write down the result.
- Revisit their answers and questions at the end of the Bitcoin Diploma.

Now that you have a clearer understanding of why money is necessary, the upcoming chapters will explore what money is, how it evolved over time, who influences it, and its newest form. Keep referring to your lists from this first day in class to draw connections between your insights and the evolution of money's creation, definition, and usage over time.

Chapter #2

What Is Money?

2.0 Introduction
Activity: Class Discussion — What Is Money?
2.1 Definition of Money
2.2 Function of Money
2.3 Properties of Money
2.4 Types of Money
2.5 The Psychology of Money: Scarcity, Time Preference, and Trade-Offs
Activity: Time Preference

Student Workbook

English Version | 2025

What Is Money?

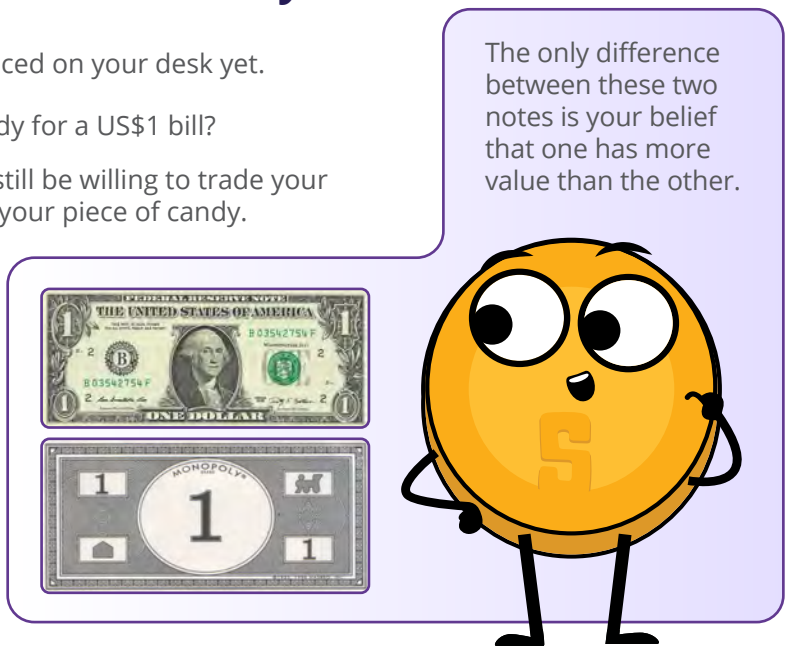
2.0 Introduction

> Money is a guarantee that we may have what we want in the future. Though we need nothing at the moment, it ensures the possibility of satisfying a new desire when it arises.
>
> **Aristotle**

Building upon our exploration of the necessity of money, this chapter explores the core question: What is money? We'll start off with a group discussion and activity.

Activity: Class Discussion — What is Money?

- Please do not eat the piece of candy placed on your desk yet.
- Who would be willing to trade their candy for a US$1 bill?
- Now, keep your hands up if you would still be willing to trade your candy for a $1 monopoly bill instead of your piece of candy.
- Why or why not?
- What makes one bill so desirable and another one as good as trash?
- What gives money its "value"?
- Where does money come from, and who decides how much of it to print?
- Why not print more money and distribute it among everyone equally?



2.1 Definition of Money

Have you ever stopped to think about what money really is? Ever wonder what makes money...well, money? Most of us know how to use it, but not many of us understand where it comes from or how it works. Money is essentially a way to exchange goods and services. It represents the value of these items in a form that can be easily traded. This can take many different forms, such as paper notes, metal coins, and electronic payments. Governments or other authorities typically issue and control money, but money is so much more than just a physical or digital medium of exchange; it's like a universal language that allows us to trade with people all around the world, even if we don't speak the same language or have the same culture. For example, you can be on the other side of the world and still "speak" money by placing a product on the counter and exchanging it for the local currency or using a credit card.

Money is like a social contract that allows us to make exchanges without having to rely on bartering or finding someone who specifically wants what we have to offer. If a group of people started accepting chocolate as payment for most goods and services, chocolate would become money (although, since it would melt in some parts of the world, we might consider it bad money).

As French economist Jean-Baptiste Say pointed out, "Money performs but a momentary function in an exchange; and when the transaction is finally closed, it will always be found that one kind of commodity has been exchanged for another."

In other words, money itself doesn't have the power to satisfy human wants; it's just a tool that allows us to trade one commodity for another.

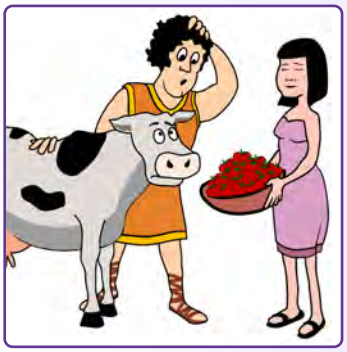
A transaction is an exchange or transfer of goods and services. It is a way of exchanging value between two or more parties.

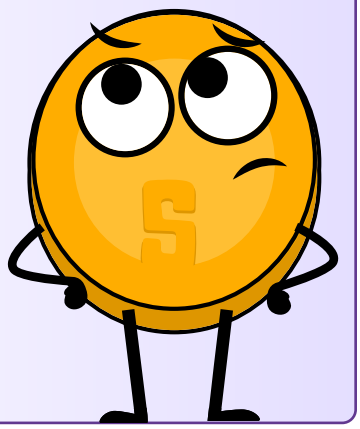
There are many different types of transactions, ranging from simple exchanges (such as buying a sandwich at a deli) to more complex financial transactions (such as buying a house or investing in stocks or bonds). Transactions can be conducted in person, over the phone, online, or through other means, and they can involve a wide range of parties, including individuals, businesses, and financial institutions.

Without money, how easy or feasible would this trade be?

Would you trade one cow for 1 Million strawberries?

Or 600,000 strawberries? How about 50,000?





Check out this short video!

Money **IS** the value **BY** which goods are exchanged.
Money **IS NOT** the value **FOR** which goods are exchanged.

In summary, money:

Facilitates trade because everyone accepts it as final payment. It also allows us to measure value and compare different goods and services. Next, we'll look at the function of money.

What Is Money?

2.2 Function of Money

When it comes to buying and selling goods and services, money is the key player. Money serves several important functions in the world, like:

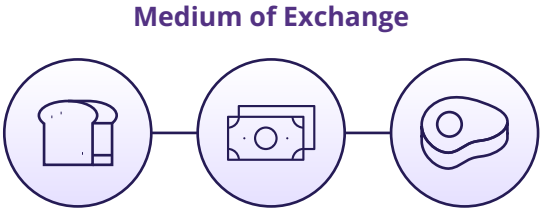
1 Store of Value

Money should maintain its value over time, making it useful as a method to save and invest the value of human labor. This lets people use money to plan for the future and borrow and lend money. So, the next time you're saving up for something special, remember that money is more than just a way to pay for things — it's a tool to help you plan and invest in your future.

What's your store of value?		BTC (USD)	Gold (USD)	USD (EUR)
	March 14, 2019	$3,846	$1,293	€0.8817
	March 14, 2020	$5,258	$1,529	€0.90056
	Gain/Loss	+36.71%	+18.25%	+2.14%

2 Medium of Exchange

With money, you don't have to find someone who wants exactly what you have to trade. Instead, you can use money to buy and sell anything you want. This makes trading and commerce much more convenient and efficient.



3 Unit of Account

Money provides a universal standard of value that allows people to express and compare the price of different goods and services. This allows for a more efficient and transparent market, where people can make informed decisions about what to buy and sell.

Unit of Account

Consumers know the value of something when you assign a price (monetary value) to it.

Think of it like this: if you wanted to buy a new car, you could compare prices from different dealerships and make an informed decision about which one to buy based on the price in dollars. Without a unit of account, you'd have to try to compare the value of one car to another using something else, like the number of cows it was worth or the length of time it took to make the car.

These three functions are what allow economies to become complex and dynamic. Without money, it would be much harder to buy and sell goods and services, and our economy would be much less developed.

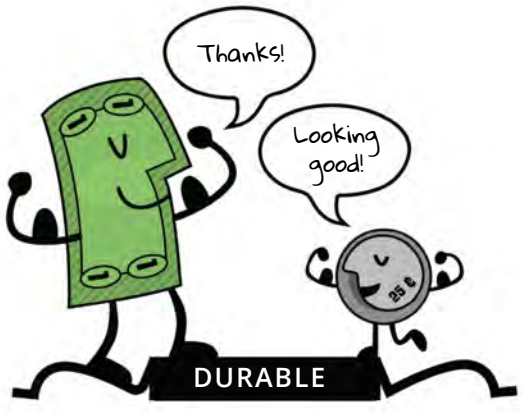
Class Exercise — What function of money is this an example of?

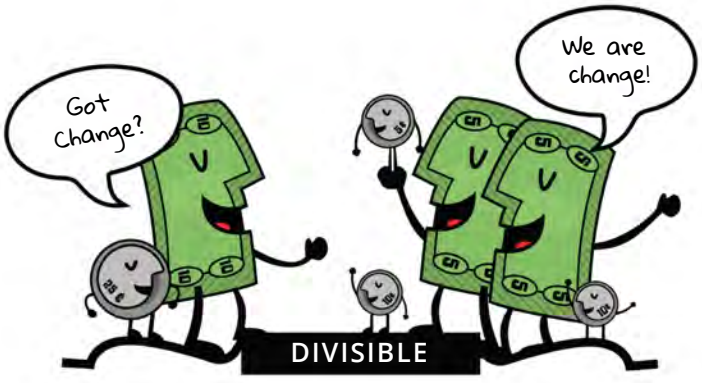
- Evan decided to save a portion of his weekly paychecks to buy a puppy.
- Adam buys two slices of pizza for $8.30 at Ray's Pizza.
- Marc can't decide whether to buy concert tickets for $75 or buy a ski pass for $95.

2.3 Properties of Money

Over time, people have ultimately realized that money must possess certain qualities to be effective as a medium of exchange. These characteristics include durability, divisibility, portability, acceptability, scarcity, and fungibility.

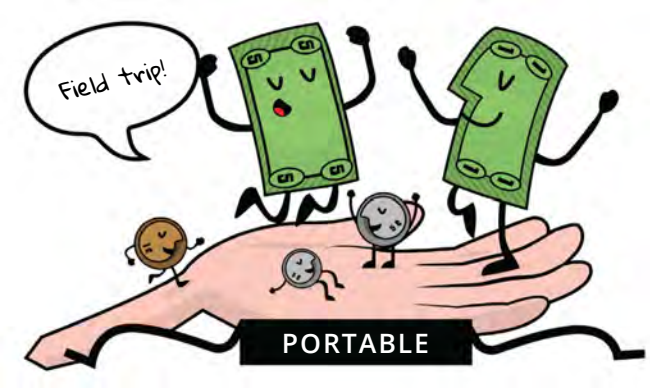
- **Durability** refers to money's ability to resist physical deterioration and last over time. This ensures that money can circulate in the economy in an acceptable and recognizable state. Gold is a durable material that can withstand wear and tear, making it a good representation of money's durability characteristic.
- **Divisibility** refers to money's ability to be divided into smaller units so that people can use it to make purchases of varying amounts. Paper bills can be easily divided into smaller denominations, making them a good representation of money's divisibility characteristic.





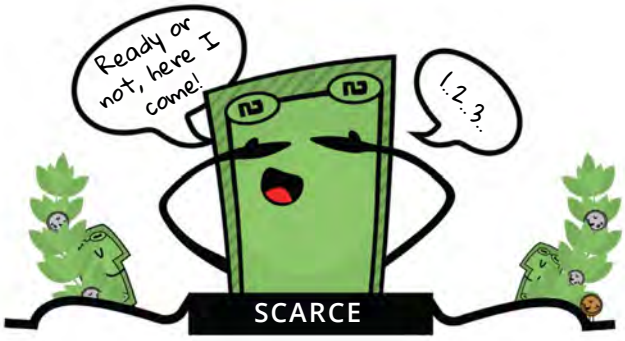
What Is Money?

Portability refers to the ease with which money can be transported and carried around. This allows people to use money to buy and sell goods and services without difficulty. Credit cards are portable, as they can easily be carried in a wallet or purse, making them a good representation of money's portability characteristic.

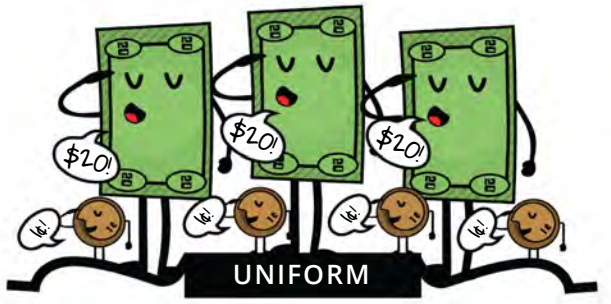


Acceptability refers to the widespread acceptance of money as a form of payment so that people can use it to buy and sell goods and services with confidence. The US dollar is widely accepted as a form of payment, making it a good representation of money's acceptability characteristic.

Scarcity refers to the limited supply of money, which helps maintain its value and prevents us from having to spend more money to buy the same amount of goods. Collectible stamps, especially rare and valuable ones, can be a good form of money because they are scarce and can appreciate in value over time. Stamp collectors often use their stamps as a way to invest their wealth and diversify their portfolio.



Fungibility refers to the interchangeability of money so that one unit of money is equivalent to another unit of the same value. Money should be uniform. Copper coins are uniform in size and weight, making them a good representation of money's uniformity characteristic. One cent is always one cent.



Overall, these characteristics make money a useful and effective tool for facilitating trade and commerce, and they are essential for economic development and stability.

Class Exercise

Different assets have different properties and perform the functions of money to varying degrees. Society ultimately determines which asset is used as money based on factors such as stability, scarcity, divisibility, transferability, and acceptance as a medium of exchange.

To determine how well different items fit the specific characteristics of money, you can score each item on a scale from **1 to 5** for each characteristic. By tallying up the scores for each item, you can determine which one is best suited to be a form of money.

[0 = Terrible; 3 = Okay; 5 = Excellent]

*** Please do not fill in the column for Bitcoin; we will return to it later in the course.**

Use the following questions to help determine how well the different items in the table fit the characteristics of money.

- **Durability:** Can the money withstand wear and tear over time?
- **Portability:** Can the money be easily transported and used in different locations?
- **Fungibility:** Is the money interchangeable with other forms of money?
- **Acceptability:** Is the money widely accepted as a form of payment?
- **Scarcity:** Is the money scarce and not too abundant?
- **Divisibility:** Can the money be divided into smaller units for transactions?

Characteristic of Good Money	Cows	Cigarettes	Diamonds	Euros	Bitcoin
Durable					
Portable					
Uniform					
Acceptable					
Scarce					
Divisible					
Total					

What Is Money?

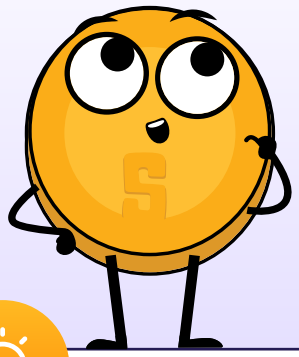
2.4 Types of Money

Money can be divided into two main categories: physical and digital.

Physical money includes:

- Fiat money, which is the paper bills and coins issued by governments and accepted as a medium of exchange.
- Representative money, which represents a claim on a physical commodity.
- Commodity money, which is a physical object that has intrinsic value and is widely accepted as a medium of exchange — for example, gold and silver.

Not all money is the same!



Commodity Money

Objects like this gun powder once served as commodity money.

Representative Money

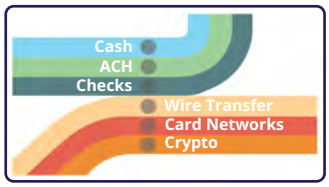
Representative money like this silver certificate could be exchanged for silver.

Fiat Money

Today, Federal Reserve notes are fiat money, decreed by the federal government to be an acceptable way to pay debts.

Digital currencies, on the other hand, can be used for online transactions and include electronic currencies, stablecoins, and cryptocurrencies.

Electronic currencies are digital versions of regular money, like dollars or euros, and can be used to buy and sell things online via digital **payment rails.**



Payment rails are the infrastructure enabling the movement of electronic currencies and other digital assets from one place to another. However, in the traditional financial system, there is always a middleman, such as a bank or other financial institution, that charges a fee and has the authority to accept, cancel, revert, or delay transactions.

In the intermediated financial system, the main types of digital payment rails include card networks — which facilitate the transfer of funds between financial institutions and merchants when a customer makes a purchase using a debit or credit card — and digital wallets, which are online accounts that allow users to store and manage their electronic currencies and make payments by transferring funds from their account to the recipient's account.

Central Bank Digital Currencies (CBDCs)

Digital versions of a country's fiat currency, which are issued and backed by the central bank and intermediated by the government.

Stablecoins

Digital currencies designed to maintain a stable value relative to an asset, like the US dollar.

Cryptocurrencies

A type of digital currency. Some cryptocurrencies are decentralized and governed by rules, while others are centralized and controlled by a small group of people.

Ultimately, a currency that operates without intermediaries is more efficient and beneficial for society, as it prevents a few individuals from controlling the money supply and concentrating their power. However, creating such a currency that facilitates secure transactions without relying on trust between parties has been a challenge throughout history. To achieve this, a currency must be created that operates like the internet, where control is distributed among everyone and no one at the same time. This requires the agreement of all parties, including those who hold power, to relinquish control for the greater good.

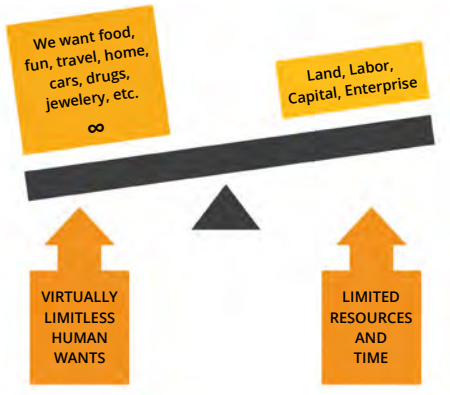
2.5 The Psychology of Money: Scarcity, Time Preference, and Trade-Offs

Imagine you are stranded in a desert and you only have one bottle of water left. You are thirsty and desperate for a drink, but you also know that you will need the water to survive until you can find more. This is a classic example of scarcity — you only have a limited amount of a resource (water) and you must make a choice about how to use it. In this situation, you might decide to ration it and take small sips over a longer period of time to make it last as long as possible.

What Is Money?

Scarcity forces us to weigh the pros and cons of how we use our resources and make trade-offs.

Alternatively, you might decide to drink as much as you can in one go, hoping that the burst of hydration will give you the energy you need to find more water. Regardless of which choice you make, you are faced with a difficult decision. In this case, the choice is between quenching your immediate thirst and conserving the water for later. This concept of scarcity applies to all kinds of resources, not just water. Whether it's money, time, or even love and attention, we are constantly faced with choices about how to allocate our limited resources.



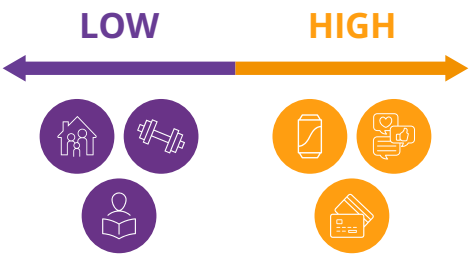
There are two types of scarcity: human-made and natural.

- Human-made scarcity, also known as centralized scarcity, includes things like limited edition designer bags, rare sports cards, and numbered art pieces. These can be easily replicated or counterfeited.
- Natural scarcity, also known as decentralized scarcity, includes things like salt, shells, and precious metals like gold. These are harder to replicate or counterfeit. The main difference between the two is control.

Centralized scarcity is controlled by a single entity, like a company or government, while decentralized scarcity is not controlled by anyone. An example of centralized scarcity that disproportionately affects the poor is the control of essential resources like clean water. In some regions, access to clean water is managed by private companies or government entities that may limit its distribution, leading the a scarcity of this vital resource. This centralized control can result in price increases or unequal access to clean water, with impoverished communities often bearing the brunt of the impact. Limited access to clean water not only affects their health and well-being but also perpetuates poverty as they may be forced to pay higher prices for water or travel long distances to obtain it.

Scarcity affects our choices. Understanding it can improve our decision-making. We often have to choose between immediate gains and long-term benefits, and these trade-offs shape our path to achieving our goals.

Time preference refers to the idea that people generally prefer to have something NOW rather than later.



An example of time preference:

Let's say you have the option to receive $100 today or $110 in a year. If you have a high time preference, you might choose to receive the $100 today because you value having the $100 now more than the benefits of waiting a year for the extra $10. On the other hand, if you have a low time preference, you'll prefer to wait for the larger reward because you are more focused on long-term planning and less concerned with immediate gratification.

Activity: Time Preference

High Time Preference vs. Low Time Preference

1. Listen to the teacher's explanation of the candy choice.
2. Decide whether you would like to receive a small candy or marshmallow now or wait until the end of the class to receive two candies or a larger, more desirable candy.
3. Commit to your decision and let the teacher know your choice. Receive your candy either immediately or at the end of the class, based on your decision.
4. Participate in the class discussion about the activity, reflecting on your decision-making process and the concept of time preference.

Conclusion and Discussion:

- What factors influenced your decision to take the candy now or wait for a larger reward later?
- How do you feel about your decision now that the activity is over?
- Can you think of real-life examples where high time preference might be harmful and where low time preference might be beneficial?
- What are some potential consequences of choosing high time preference over low time preference?

In the context of the desert example, this means that you might be more inclined to drink all the water right away, even if it means that you won't have any left for later. This is because the thirst you feel right now is more pressing than the potential thirst you might feel in the future.

On the other hand, if you choose to ration the water and drink it slowly over time, you are demonstrating a lower time preference. This means that you are willing to wait to satisfy your thirst and improve your chances of survival. The concept of opportunity cost is closely related to the idea of scarcity and time preference.

What Is Money?

Opportunity cost refers to the value of the next best alternative that you give up when you make a decision. **Every decision involves trade-offs.**

Today's Choice	Now	Later
	  	  
Buying a $7 strawberry smoothie	Spending $7 another way	Benefiting from regularly saving $7

In the desert example, the opportunity cost of drinking all the water right away is the survival benefits you would have gained from rationing the water and using it over a longer period of time.

Let's say you decide to ration the water and take small sips over a longer period of time. As a result, you have the energy and hydration you need to search for more water. However, while you are searching, you come across a cactus that has a small amount of water inside. It's not a lot, but it's enough to quench your thirst for the moment. If you had decided to drink all of your water at once, you might not have had the energy to search for more water and come across the cactus.

In this case, the opportunity cost of drinking all of your water at once would have been the chance to find the cactus and get more hydration.

This example illustrates how opportunity cost involves not just the immediate trade-off between two options but also the potential future opportunities that may be gained or lost as a result of our choices.

Our willingness to give up a larger reward in the future in exchange for a smaller reward now is influenced by our time preference, or how much we value immediate gratification versus long-term planning.

In this chapter, we explored the fundamental concept of money, covering its definition, functions, properties, and various types. An essential aspect of our discussion involved understanding the psychology of money, focusing on concepts like scarcity, time preference, and trade-offs. This exploration laid the groundwork for comprehending the complicated nature of money and its role in our lives. In the next chapter, we'll talk about the history of money and how it has evolved over time.

Chapter #3

The History of Money

3.0 Introduction

Activity: Barter Game

3.1 Evolution from Barter to Modern Currency

3.1.1 Problems with Early Forms of Money

3.1.2 Development of Coinage and Paper Money

3.1.3 Transition from Sound to Unsound Money

3.1.4 Paper to Plastic

3.2 Digital Currency

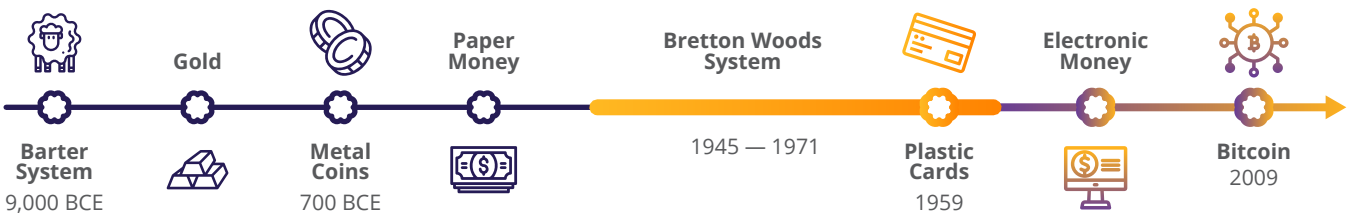
Student Workbook

English Version | 2025

The History of Money

3.0 Introduction

> Money was not evolved by design but arose out of the market process. It was not created by governments. It emerged over time as a spontaneous order.
>
> **Murray Rothbard**



Imagine a time long ago when people didn't have the coins or paper bills we use today. Back then, they had a unique way of trading things — using items like shells or precious metals like gold as a kind of special currency. This might sound strange, but it was their version of money, something everyone agreed had value. In this chapter, we will embark on a journey through time, experiencing the evolution of money firsthand. We'll trace its origins and observe how it has changed and adapted through history.

Activity: Class Exercise — Barter Game

Your teacher has given you a small piece of paper. Your goal is to trade what you "have" for what you "want" in a game of commerce throughout history. Please write your name at the top of the paper in small, legible letters.

Round #1: Barter

It is the year 6000 BCE. Needless to say, money as we know it has not been invented. You are in Mesopotamia and directly exchange goods and services with one another through **bartering**.

> As a side note, many businesses that still accept non monetary payments for their services and governments treat these bartered transactions the same as currency transactions for tax-reporting purposes.

Cut your sheet of paper at the dashed line. Your goal is to trade away your "have" as many times as you need to finally get your original "want." You cannot change your original "want." You will have five minutes to accomplish the goal of this exercise.

When your new "have" matches your original "want," return to your seat. After the time is up, if you have not found a trading partner, return to your seat anyway.

Raise your hand if you were able to get what you wanted after one trade. Two? Three?

Answer the following questions briefly but substantially:

1. Why were some of you able to get someone to trade with while others were not?

2. What are the benefits of bartering?

3. Based on your experience with this exercise, what are the drawbacks of bartering?

Round #2: Commodity Money

Fast-forward and travel to the western coast of Africa sometime around the 14th century BCE. Bartering has become tedious and inefficient. We have evolved as a civilization and are now using **commodity money.**

Cowry Shells to Coins

1300 BCE

1000 BCE

687 BCE

FUN FACT
Cowry shells were accepted as legal tender in some parts of Africa until the 20th century.

These proto-coins were oval-shaped, made from "electrum" (a gold/silver alloy), and had a design on one side only.

1300 BCE
Cowry shells are the predominant form of payment in most of Asia, Africa, Oceania, and some parts of Europe.

1000 BCE
China's Western Zhou dynasty begins using metal coins.

687 BCE
King Alyattes of Lydia (present-day Turkey) orders the first metal coins to be minted in the Western world.

The History of Money

Your teacher has given you one macaroni (or a printed image of a macaroni). For simplicity, let's assume the price of each good is one macaroni.

Your goal again is to obtain what you "want," but now, our species has smartened up a bit and found a way to solve certain problems.

- Why do we consider macaroni commodity money?
- How do we get the things we want now?
- Was the macaroni round easier?
- Why do you think money has replaced commodities?
- In what ways is using commodity money more efficient than bartering?
- What are the drawbacks to using macaroni as money?
- What do you think happened when Spain started to bring back boatloads of macaroni into your community (gold and silver from the Americas back to Spain)?

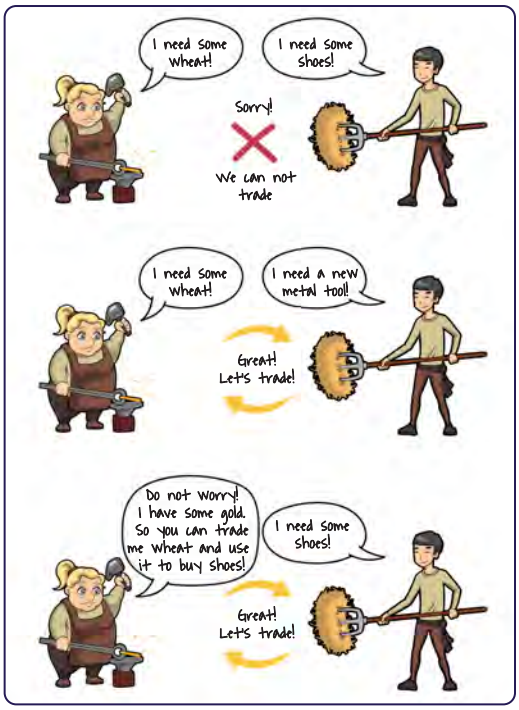
3.1 Evolution from Bartering to Modern Currency

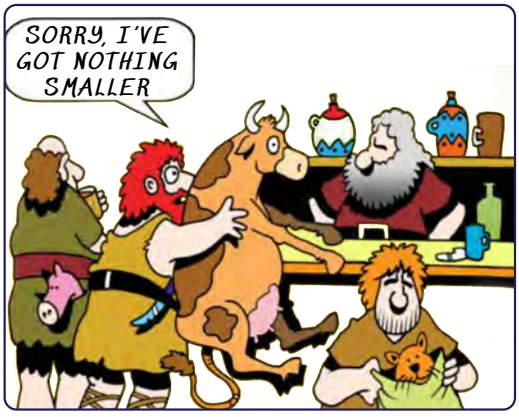
3.1.1 Problems with Early Forms of Money

Watch this short video to learn about the "Origins of Exchange", in the series "The History of Paper Money."

In barter economies, people trade with each other based on the relative value of the goods and services they have to offer. Barter economies are inefficient and can be difficult to manage, especially in complex societies.

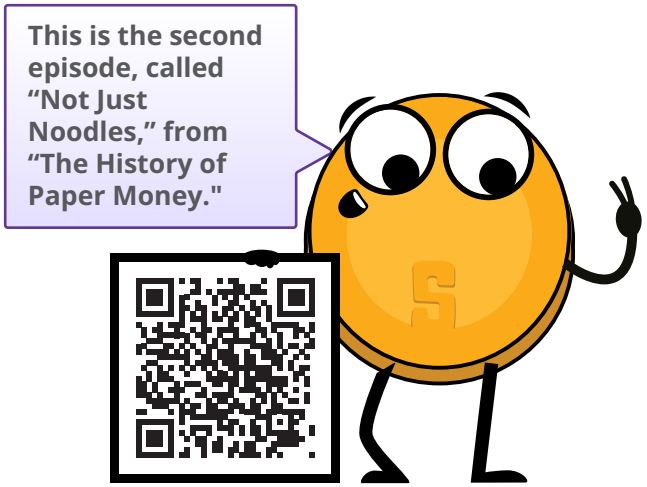
A situation like the **double coincidence** of wants is necessary in any bartering system, since people must always find someone who has what they want but who also wants what they have to offer in exchange.





Let's suppose:

- Joseph wants to trade his banana for Yael's coconut.
- But Yael only wants to trade her coconut for Tammy's mango.
- And Tammy only wants to trade her mango for Joseph's banana.
- They are stuck in a never-ending cycle of fruit-trading without a double coincidence of wants.
- Joseph suggests they just trade their fruits for a nice cold soda, but they realize they are on a remote island and there is no soda.
- They decide to just sit on the beach and enjoy their fruits in silence.

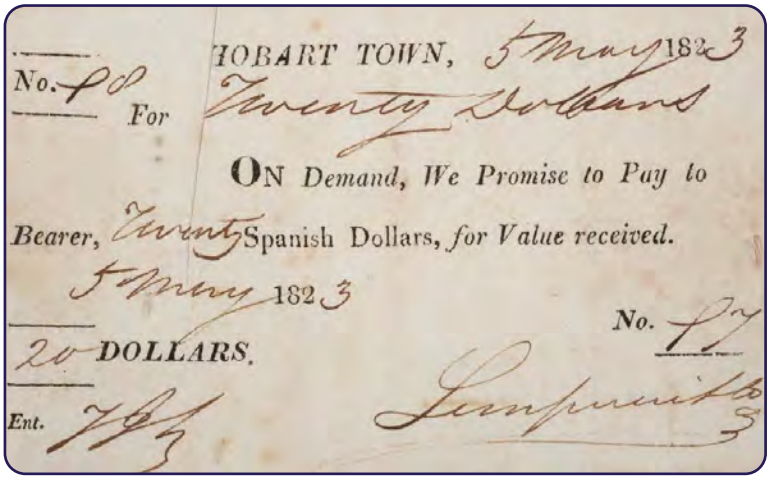


3.1.2 Development of Coinage and Paper Money

As you and your community become more involved in trade and commerce, you realize the limitations of using bartering and other forms of non monetary exchange. You decide to adopt the use of metal coins as a form of money.

Commodity money is money made from valuable metal materials like gold and silver. These have historically been used as a store of value, a medium of exchange and, in the distant past, a unit of account.

The History of Money



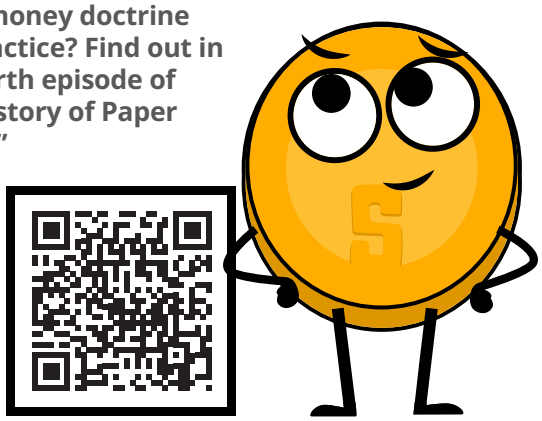
However, as you begin to use metal coins more frequently, you encounter some drawbacks. They can be heavy and inconvenient to carry in large transactions, and you notice that some people are taking advantage of the system by melting down the coins and creating new ones by mixing them with cheaper metals, which causes prices to rise and undermines trust in the system.

In an effort to address these issues, you and your community start to use paper receipts as a form of money. These paper receipts, which have their origins in Ancient China, are a convenient and easily exchangeable form of currency. They are backed by gold and other valuable metals and can be converted into these metals, as they were from the 17th to the 19th century. This allows you to have a more portable, easily transferable form of money while still maintaining the value and security of precious metals.

3.1.3 Transition from Sound to Unsound Money

Fast-forward to the 17th century in Sweden. Now, you are completely dependent on banks to store your valuable assets. However, you start to notice something fishy going on with these bankers; it seems they are issuing more paper receipts than they have gold in storage, allowing them to create more money than they have assets to back it up. This sneaky practice allows bankers to profit from the difference between the value of the paper receipts and the value of the gold they are holding for their customers.

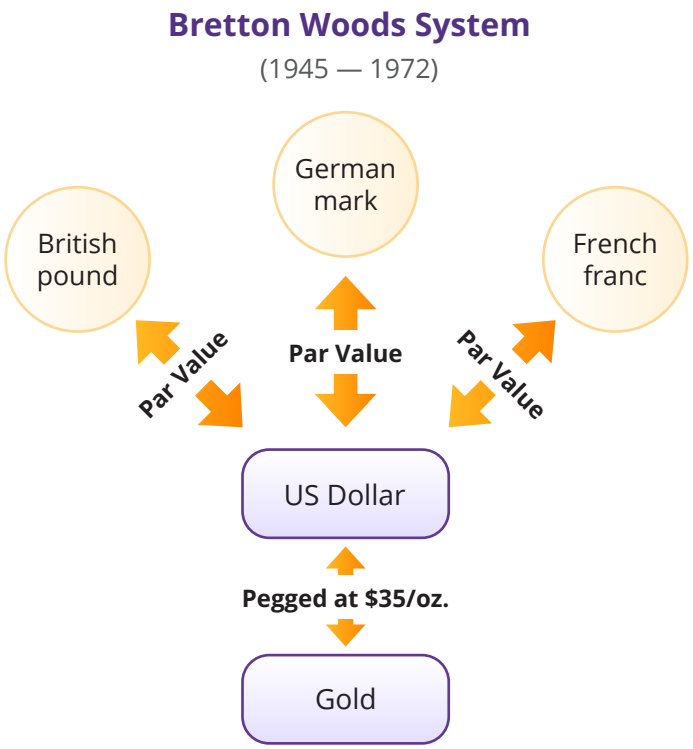
What happens when you really try to put the paper money doctrine into practice? Find out in the fourth episode of "The History of Paper Money."



You realize that this marks a major shift in the way money works. You are moving from a system of sound money (i.e. money backed by precious metals) to a system of unsound money (i.e. fiat currency not backed by a physical commodity). This transition didn't happen overnight but rather was a gradual process influenced by several factors. The industrial revolution, with its mass production and urbanization, played a role, as did the growth of advanced financial systems like banks and stock markets. The emergence of central banks and other monetary authorities contributed to the centralization or the control of money, leading to the issuance of fiat currencies to support economic growth.

However, you also begin to see the **downsides of this centralization**, including irresponsible consumption, **increased debt**, and manipulation of citizens through economic incentives.

Until World War I, you were able to convert your paper money into a preset amount of gold. However, the two world wars and the 1929 economic crisis put an end to that. In 1944, the Bretton Woods agreement was signed, establishing the U.S. dollar as the world's reserve currency and fixing the value of the U.S. dollar to the price of gold at a rate of $35 per ounce. Other countries' currencies are pegged to the dollar, which helps stabilize international financial markets.



Unfortunately, the system began to break down in the late 1960s, leading to the Nixon Shock in 1971, when the US government suspended the dollar's convertibility into gold. This marked the end of the gold standard and the beginning of a world driven by the creation and accumulation of debt.

As you go about your daily life, you begin to notice that the value of money is no longer as stable as it used to be. Just like a flexible ruler makes it difficult to accurately measure the length of a table, living in a fiat world where the value of money is subject to the unpredictability of those in power can also make it difficult to accurately measure the value of goods and services. You feel confusion and unease adjusting to a world where the value of money is no longer tied to a physical commodity like gold.

You see the impacts of this shift on the global economy and start to question the stability and reliability of fiat currencies. You realize that, in this modern world, the dollar is no longer fixed and consistent as it was when it was pegged to gold but instead becomes subject to fluctuation. This makes it more difficult to use the dollar as a unit of account, as its value is affected by various factors including inflation (rising prices), interest rates, the strength of the country's economy, political events, market speculation, and demand in international trade. It can be a confusing and unpredictable time as you try to navigate the constantly shifting value of the dollar and its impact on your daily life.

Despite efforts to improve quality of life through modern monetary systems, increased efficiency, greater access to information, and enhanced communication, the majority of people's standards of living begin to decline due to:

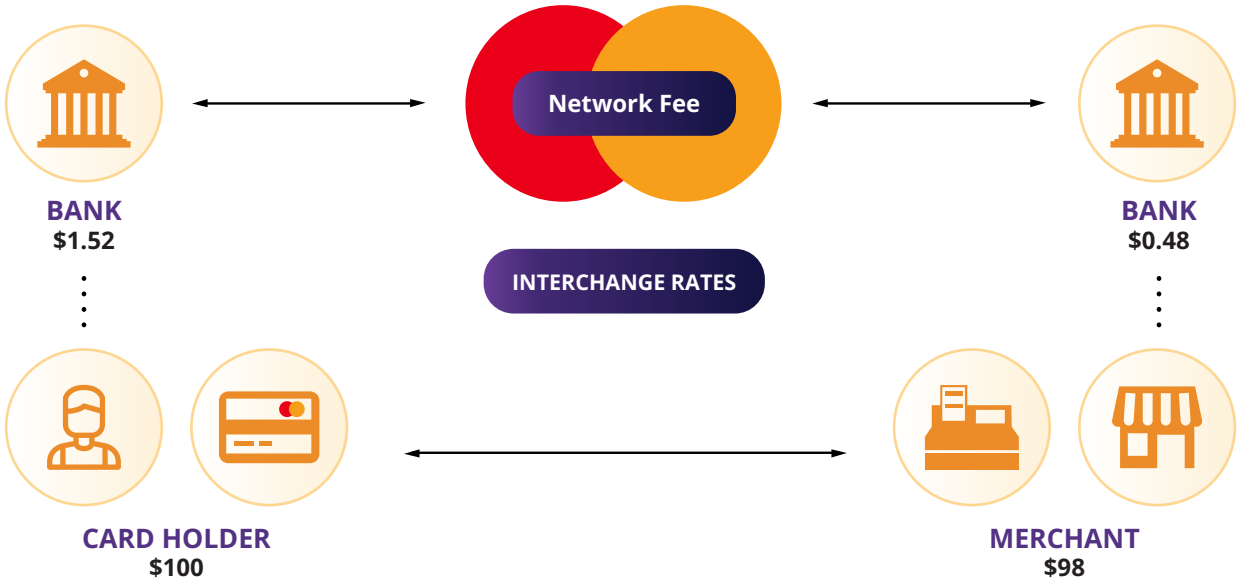
- Abuse of centralization
- Rising prices
- Stagnation real wages
- Weakening currencies
- The need to spend more money for fewer things

This creates challenges for those with lower economic resources who may have limited access to education, credit, resources, social networks, and political representation, leading to potential disadvantages in their ability to succeed.

As a result, the rich seem to keep getting richer and the poor seem to keep getting poorer.

3.1.4 Paper to Plastic

Today, we've come a long way from the introduction of the first credit card back in the 1950s. With a simple swipe of plastic, we can buy whatever we want, whenever we want, without any hassle. It's like opening up a world of endless possibilities, and the excitement of discovering what it holds is palpable... or so we thought. Little did we know that our reliance on credit would have painful aftereffects — like raising the overall cost of goods and incentivizing a certain economy doomed to fail.



As technology advances, so does the way we handle money. The internet has become a major player in the financial world, with online banking and e-commerce websites making it possible to manage and spend money entirely online.

The rise of digital money marks the next significant leap in this evolution, offering new possibilities and reshaping the way we make financial transactions.

3.2 Digital Currency

Unlike traditional ones, digital currencies exist solely in electronic form. They are stored and exchanged using computers and special software.

Digital currency allows individuals to send their money through the internet. Much like how email allows us to send messages instantly and without shipping costs, digital currencies allow us to send and receive value instantaneously and at very little cost.

The currencies we use today are becoming more and more digital. Only a small fraction of the money supply exists in the form of coins and paper bills. Banks and banking services provide their users with applications to seamlessly exchange money over the internet. But where is the money coming from?

In this chapter, we've witnessed the transformation from sound money, represented by gold, to unsound money in the form of paper, and now, digital fiat currency. In the next chapter, we'll explore how the current fiat monetary system works and how it came to be.

Chapter #4

What Is Fiat Money and Who Controls It?

4.0 Introduction

4.1 Brief History of Fiat Money

4.2 The Fiat System

- **4.2.1** A Monetary System by Decree
- **4.2.2** Fractional Reserve Banking: A System Fueled by Debt
- **Activity:** Fractional Reserve Banking
- **4.2.3** Who Controls the Fiat System and How Do They Benefit?

4.3 Central Bank Digital Currencies: The Future of Fiat Money

Student Workbook

English Version | 2025

What is Fiat Money and Who Controls it?

4.0 Introduction

> The history of mankind is the history of money losing value.
>
> **Milton Friedman**

We saw in the previous chapter how money evolved over time and how our monetary system transitioned from sound to unsound money, shaping the world we live in today. This chapter dives deeper into how these developments led to today's fiat system and how that fiat system works.

So, what does this fiat system look like, and how did it come into existence?

To answer this question, we need to begin by centering our attention on the US dollar, the world's current reserve currency, which plays a dominant role in today's world. Every country, directly or indirectly, feels the impact of the decisions made regarding the US dollar. To truly understand how the fiat system operates in your country, it is essential to unravel the historical threads that connect it to the fiat system's birthplace — the United States of America.

4.1 Brief History of Fiat Money

1815-1933	1913	1933	1934	1944	1971	1980
Gold Standard	Creation of the Central Bank called "The Federal Reserve"	Executive Order 6102. Every citizen was obliged to turn in their gold at an exchange rate of $20.67 per ounce	Gold Reserve Act. Stealing wealth from the people by devaluing the dollar by 40% to $35 per ounce of gold	Bretton Woods Agreement: USD became the dominant world reserve currency	Nixon Shock, which gave birth to the fiat system by ending the redeemability of U.S. dollars for gold	Value of gold increased from $35 per ounce in 1970 to $870 per ounce in 1980, which caused people's money to lose 96% of its value in just 10 years

Timeline Visual

In the 19th century, civilizations worldwide thrived on a sound money standard, using precious metals like gold and silver due to their scarcity, durability, and recognizability. As global trade grew, carrying large amounts of metal became challenging, leading to the emergence of gold and silver warehouses. These warehouses securely stored people's valuable metals and provided paper certificates redeemable for specific amounts of gold or silver. In exchange for depositing their money, individuals received paper

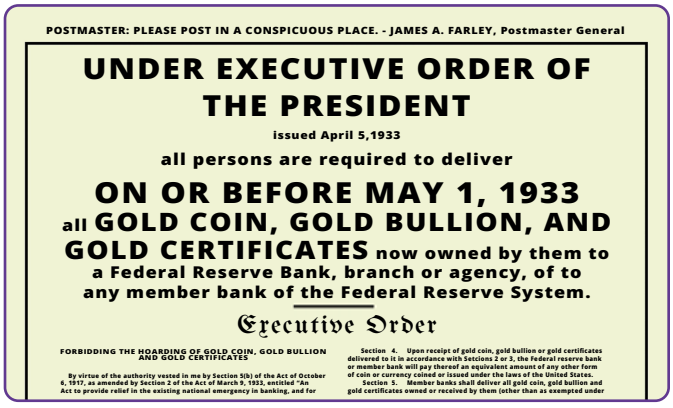
certificates directly tied to the exact amount of gold or silver they stored. This direct link between paper certificates and tangible commodity money marked the early stages of what we now recognize as banks.

Initially, banks aimed to safeguard clients' money but later engaged in risky lending practices, issuing certificates for gold they didn't have. This practice posed the threat of bank runs if too many clients claimed their money simultaneously. To address the risk, banks collaborated with governments to establish a

system legalizing re-lending. In 1913, they created the Federal Reserve, a central bank responsible for generating new paper certificates and bailing out troubled banks. Globally, governments recognized the value of gold and silver, leading to conflicts and wars for control. In the years leading to World War II, leaders like Lenin, Stalin, Churchill, Roosevelt, Mussolini, and Hitler seized gold for strategic purposes.

In the early 1930s, a significant change occurred in the way money was backed by assets in the United States. At that time, a lot of people's wealth was stored in the form of gold. However, in 1933, President Roosevelt issued Executive Order 6102, which demanded that every citizen give up their gold. This wasn't a voluntary exchange — people were required to surrender their gold, and if they refused, they faced severe penalties.

The government set the exchange rate at $20.67 per ounce of gold. This meant that for every ounce of gold a person had, they received paper certificates equivalent to $20.67. People had to accept these paper dollars, hoping that one day, they would be able to exchange them back for gold.



POSTMASTER: PLEASE POST IN A CONSPICUOUS PLACE. - JAMES A. FARLEY, Postmaster General

UNDER EXECUTIVE ORDER OF THE PRESIDENT

issued April 5,1933

all persons are required to deliver

ON OR BEFORE MAY 1, 1933

all **GOLD COIN, GOLD BULLION, AND GOLD CERTIFICATES** now owned by them to a Federal Reserve Bank, branch or agency, of to any member bank of the Federal Reserve System.

Executive Order

FORBIDDING THE HOARDING OF GOLD COIN, GOLD BULLION AND GOLD CERTIFICATES

By virtue of the authority vested in me by Section 5(b) of the Act of October 6, 1917, as amended by Section 2 of the Act of March 9, 1933, entitled "An Act to provide relief in the existing national emergency in banking, and for

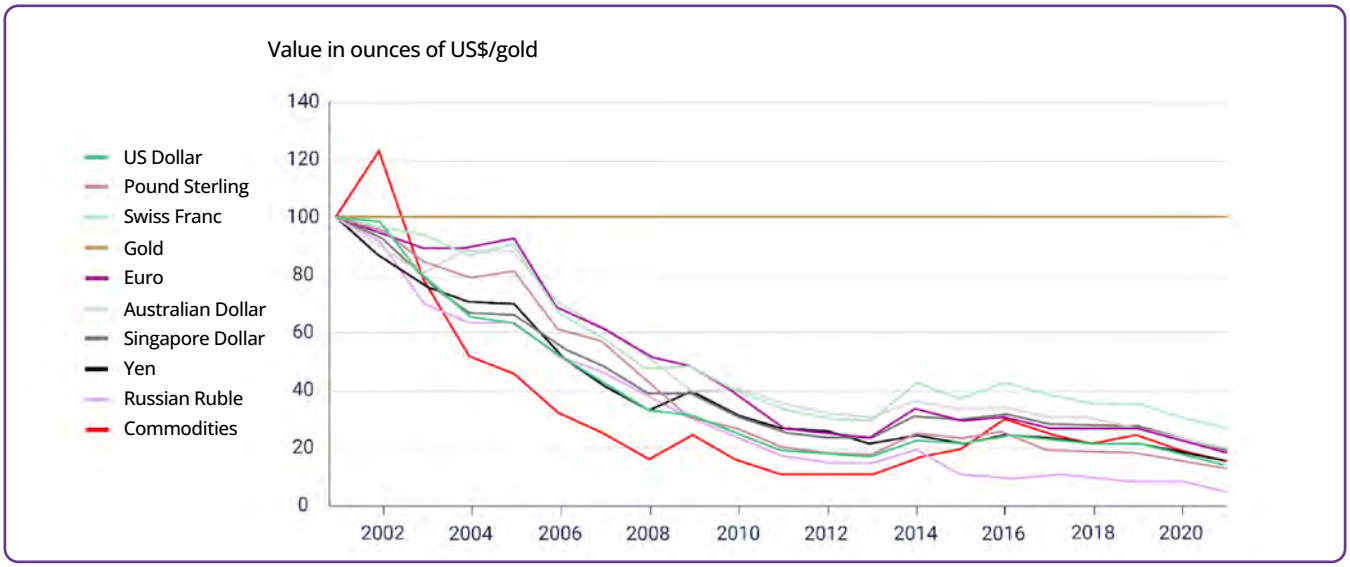
Section 4. Upon receipt of gold coin, gold bullion or gold certificates delivered to it in accordance with Sections 2 or 3, the Federal reserve bank or member bank will pay thereof an equivalent amount of any other form of coin or currency coined or issued under the laws of the United States.

Section 5. Member banks shall deliver all gold coin, gold bullion and gold certificates owned or received by them (other than as exempted under

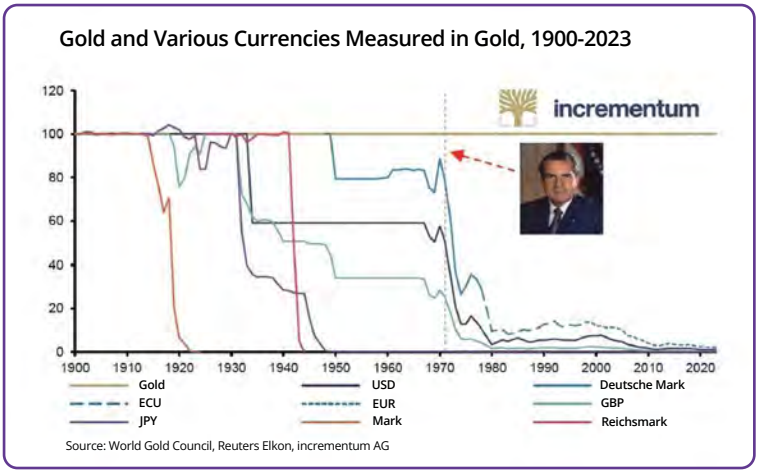
What Is Fiat Money and Who Controls It?

In 1934, the Gold Reserve Act allowed people to exchange their paper dollars for gold again. However, there was a catch: the government deliberately devalued the paper dollars by increasing the exchange rate to $35 per ounce of gold. This devaluation hit hard-working individuals in the lower and middle classes as it meant that their savings, once worth more, were now worth less due to the decrease in the value of the paper dollars.

After World War II, the Bretton Woods agreement in 1944 established that the US dollar would be the world's reserve currency, and it could be exchanged for gold. However, this link between the U.S. dollar and gold was severed in 1971 when President Nixon ended the redeemability of the U.S. dollar for gold. This marked a significant shift, leading to the adoption of a fiat money system where the value of the currency is not backed by a physical commodity like gold but rather by the trust and confidence of the people who use it. As governments and central banks retained most of the people's gold, the value of gold surged, reaching $870 per ounce in 1980.



In conclusion, the story of how human society transitioned from a sound money standard into an unsound (fiat) standard tells us how governments and banks captured precious metals from their citizens. While real money ended up in the pockets of governments and banks, the people were left with pieces of paper whose only value comes from governments mandating its use.



4.2 The Fiat System

> The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust.
>
> **Satoshi Nakamoto**

Humanity transitioned from sound money controlled by the many to unsound money controlled by the few. But how does this system work exactly?

4.2.1 A Monetary System by Decree

The fiat system is marked by its mandatory nature, imposed on people through legal tender laws. The term "fiat," originating from Latin, means "by decree," representing a directive issued by authorities.

Unlike money backed by tangible assets such as gold, fiat money lacks such support. Instead, its use is mandated by law. Everyday currencies like dollars, euros, pounds, yuans, pesos, and others fall under the category of fiat money.

Legal tender law: A law making it obligatory for all citizens to accept a specific kind of currency.

The value of fiat money is based on the belief that it can be exchanged for goods and services and the illusion that it will retain its value over time. Fiat money is comparable to a concert ticket; its value lies not in the paper ticket itself but in the assurance that the band (the government and its central bank) will deliver a great show (provide economic stability).

Pros of Fiat Money

- **Ease of use:** Fiat money is convenient for everyday transactions.
- **Lower costs and risks:** Fiat money doesn't require heavy security like gold, making it cheaper and safer.

Cons of Fiat Money

- **Inflation risks:** Prices can continuously rise, causing inflation and historical instances of hyperinflation.
- **Centralized control and manipulation:** Small groups can influence and manipulate the system, leading to censorship and confiscation.
- **Counterparty risk:** If the government faces challenges, the currency can lose value.
- **Potential for abuse:** The system can be misused, resulting in corruption and loss of trust.

What Is Fiat Money and Who Controls It?

Commodity vs. Fiat: Picture the Difference

Remember: Before fiat currency came about, governments would mint coins out of a valuable, scarce, and difficult-to-get physical commodity such as gold or silver, or they would print paper money that could be redeemed for a set amount of a physical commodity. This was the commodity-backed system.

Now, in the fiat system, it's more like having Monopoly money. Money in the fiat system consists of pieces of paper printed by the central bank, and the government's policies directly influence its value. The government and central banks are basically the "bankers of the Monopoly game" who are in control of how the game works, who gets what, and how much it is worth. In other words, the government promises to do a good job at managing the monetary system.

In conclusion, fiat currencies only have value because the government mandates their use; there is no utility to fiat money in itself.

In summary, the fiat system is a trust game where the value of our money relies on the promises of those in charge and people can only hope that their government acts for the benefit of all. Next, we'll see how banks make new money, who's involved, and how it affects the economy.

4.2.2 Fractional Reserve Banking: A System Fueled by Debt

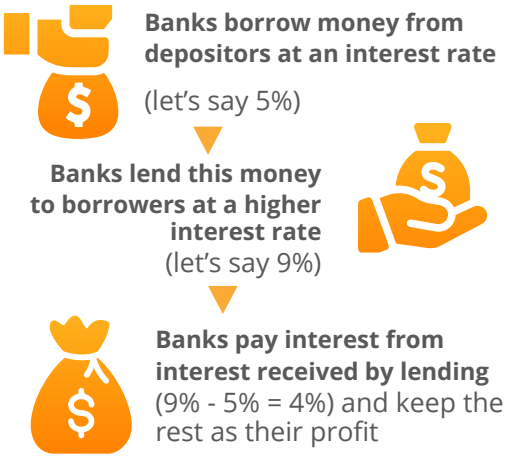
> It is well enough that people of the nation do not understand our banking and monetary system, for if they did, I believe there would be a revolution before tomorrow morning.
>
> **Henry Ford**

Fractional reserve banking is one of the main parts of the fiat system, allowing banks to lend out a significant portion of their clients' deposits. Have you ever wondered why banks offer so many services to their customers? While it may seem like they are being generous, it's important to remember that banks are businesses and their primary goal is to make a profit. But how do they make a profit if they let people borrow money?

In addition to earning interest on deposits, banks generate revenue in other ways, including:

- Charging interest on loans they give out
- Charging fees for services like ATM usage and account maintenance
- Earning money through investments, like buying and selling securities or investing in real estate
- Keeping a percentage of loans in reserve and investing or lending out the rest
- Paying interest on deposits and charging fees on checking and savings accounts

When a bank receives a deposit, it's required to keep only a fraction (reserve requirement) and can lend out the remaining portion.



For instance, if you deposit $100 with a 10% reserve requirement, the bank can lend $90, keeping only $10 as reserves. The borrower deposits $90 into another bank, allowing the cycle to continue. Despite the initial $100 deposit, the total money in the economy grows to $271, seemingly appearing out of nowhere — a phenomenon known as the multiplier effect.

This process leads to a debt-driven monetary system as banks create new currency with each loan, increasing the overall money supply. As fractional reserve banking continues, the total debt in the economy rises, contributing to inflation.

The system relies on a continuous cycle of currency creation through lending, akin to a steady supply of drugs for an addict. However, if banks lend more money than they have in reserves and depositors rush to withdraw simultaneously, banks could face failure.

Here, the central bank intervenes as a lender of last resort, providing new currency to prevent bank failures. The central bank achieves this by repurchasing assets or injecting currency directly into banks' accounts. In essence, banks are saved from failure through the constant injection of new currency by central banks. This debt-fueled system systematically rescued by the central bank results in boom and bust cycles.

Imagine you have a friend who happens to be a banker; let's call him Dax.

Dax loves bikes, and he wants to borrow your bike because he has a lot of places to go. You give him your bike, and in a twist, Dax starts to promise the same bike to lots of other friends at the same time. With your one real bike that you lend to him, Dax manages to create more imaginary bikes and starts to lend them out to friends. Each of his friends thinks they can enjoy a nice ride whenever they like. But, here's the twist — there's only one real bike! All the others are imaginary and just promises.

So, what happens? As more imaginary bikes circulate, everyone is very happy, at least initially, because in the beginning, no one uses the bike at the same moment — it looks like there is no problem; it feels like there's an abundance of bikes for everyone. So, all the friends start making more plans, thinking about all the places they'll go with their bikes.

However, here's where the magic starts to lose its charm. One sunny day, everyone decides it's a perfect day for a bike ride. They all show up at Dax's doorstep, excited to take their imaginary bikes for a spin. But, reality hits — there's only one real bike. Disappointment ensues, and suddenly, the value of the promised rides diminishes.

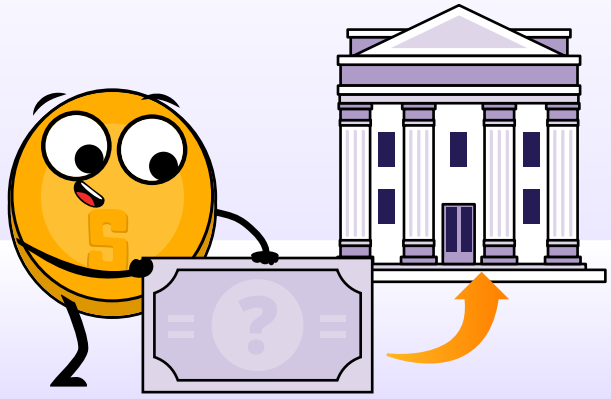
In the world of fractional reserve lending, it's a similar story. Banks lend out more money than they actually have, and for a while, everyone enjoys the benefits. More money circulates, and it seems like there's plenty to go around. But, if too many people try to withdraw their money at the same time, the true value becomes apparent: there's not enough to fulfill all the promises.

This scenario affects the common good and value of everyone involved. The promise of abundance turns into a scam. Just as the imaginary bikes lose their perceived value when everyone wants a real ride, the value of money in the economy can diminish when everyone rushes to claim their real share. When that happens, people figure out that the money they have at a bank isn't really in there, which leads to panic, bank runs, and even the collapse of entire economies. The ones who are paying for these collapses have, until now, always been the same group: the lower and middle class of the world.

What Is Fiat Money and Who Controls It?

Boom

Credit expansion via fractional reserve banking (commercial banks create fiat currency and lend it to customers)



Expansion of the money supply (the newly created currency enters the system and inflates the money supply)

Over investment (customers use the loans to invest in markets, creating a surge in demand)

Price inflation (prices rise as a result of new demand)

Lack of new demand

Bust

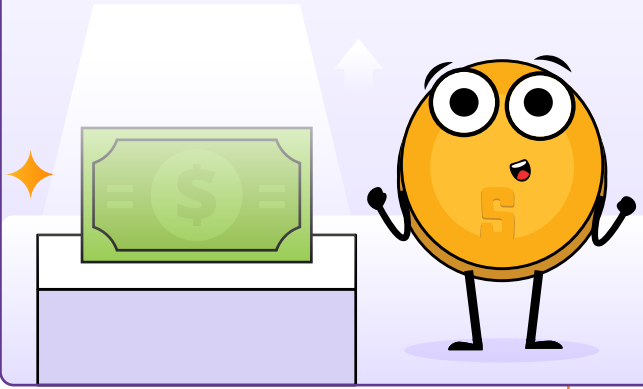
Prices fall (investors panic and begin to sell their investments at lower prices as there is no real demand for them)

Individuals and businesses default on their loans (as the value of their collateral decreases)

Banks default (as they now own assets worth less than the value of the loans they issued)

Central bank intervention, rescuing banks

Banks rescued with new currency (the central bank repurchases the assets the banks are holding at a higher price than current market valuation in order to rescue them, or directly create new currency and give it to them)



Repeat (more credit expansion, preparing for the next boom phase)

Activity: Fractional Reserve Banking

In the following exercise, we'll explore how fractional reserve banking can lead to currency debasement, inflation, and a decrease in purchasing power. We'll use a simplified example involving six participants, one of whom will act as a bank, and a reserve ratio that's still being used a lot today: 10%.

- Person A just won $100,000 from the lottery and deposits it in the bank (B). With a 10% reserve ratio, B must keep $10,000 in its vault and can lend out the remaining $90,000.
- Person C borrows the maximum amount ($90,000) from B and uses it to buy a house from D.
- Person D deposits the $90,000 received from C into the bank (B). The total deposits in the bank are now $190,000.
- Person E requests a loan from B, and the bank lends out 90% of the new deposit, which is $81,000.
- Person E uses the $81,000 loan to buy an art piece from F, who then deposits the money in the bank (B). The total deposits recorded are now $271,000.

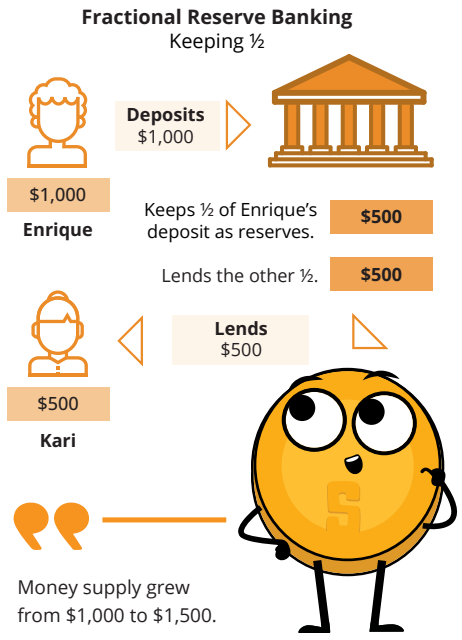
In this scenario, the initial $100,000 deposit has resulted in a total of $271,000 in deposits after circulating through the economy.

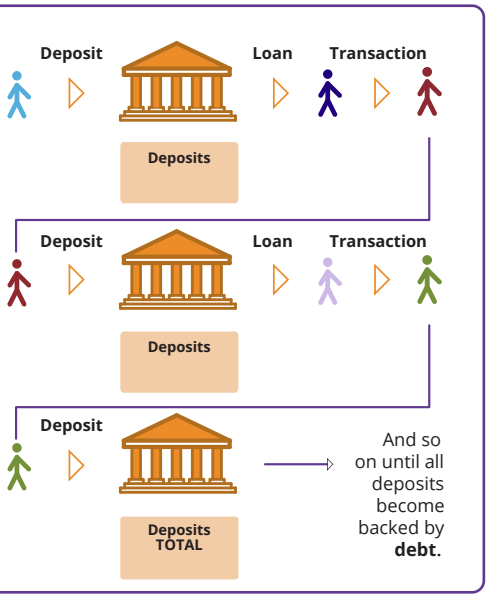
If the reserve ratio were lowered to 1%, the amount of money created would be significantly higher ($100,000 / 0.01 = $10,000,000. In this case, how much money would actually be created with those $100,000 if the money continues to circulate throughout the economy?

It's important to note that as of 2020, the Federal Reserve (the Central Bank of the USA) reduced reserve requirement ratios to 0% in order to stimulate the economy.

We need the following volunteers:

A = Depositor (Lottery Winner) (Light Blue)
B = Bank Cashier (Bank)
C = Debtor #1 (Dark Blue)
D = Property Owner/Depositor (Red)
E = Debtor #2 (Light Purple)
F = Art Gallery Owner/Depositor (Green)



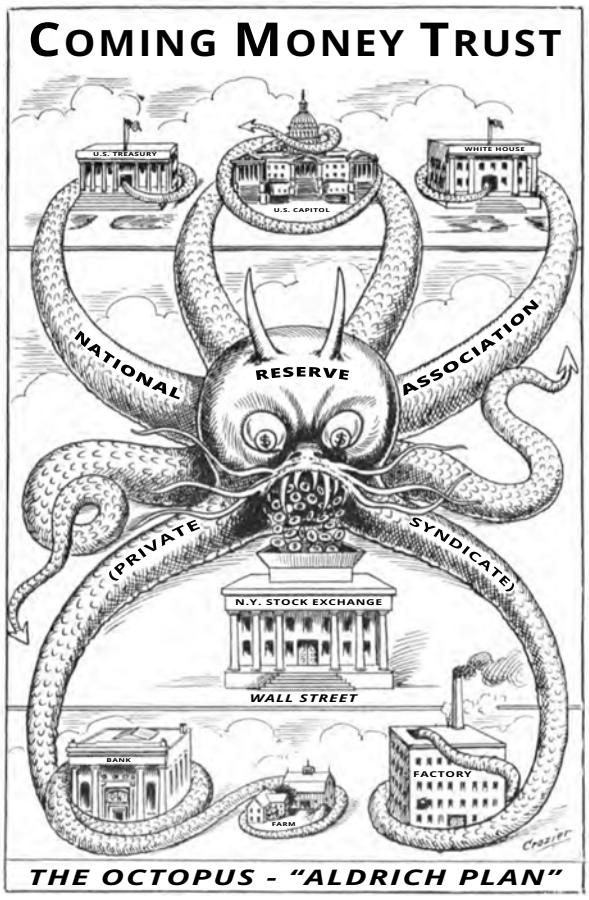


What Is Fiat Money and Who Controls It?

4.2.3 Who Controls the Fiat System and How Do They Benefit?

There are four main players: the government, wealthy individuals, the financial sector, and the central bank. Together, they control the fiat system.

- **The Government:** The government is like the director of the fiat show. Along with tax collection, it is funded through new debt (bonds) issued by the Treasury. When there is insufficient demand for these bonds, any remaining debt is purchased by the central bank. This means they can keep doing their activities and pursuing their interests without needing approval from the people. It's like getting a credit card without worrying about paying it back immediately. This might seem good for the government, but it comes at a cost for everyone else.



- **Wealthy Individuals:** Wealthy individuals benefit a lot from the fiat system. With the ability to accumulate more debt, they can invest in assets like commodities, real estate, and stocks, creating new wealth almost effortlessly.

- **Financial Sector (banks):** Banks and other financial institutions do not directly control the fiat system but greatly benefit from it. Free from accountability, they can pursue and accelerate the creation of new currency via fractional reserve lending, benefiting from higher revenue. Banks are virtually free from consequences as they are bailed out with new fiat currency to prevent the whole system from collapsing.

- **The Central Bank:** The central bank is the one pulling the strings, supposedly controlling the growth of the money supply. But here's the trick — the central bank is also subject to the government's laws, serving the government's interests. It's like a puppeteer being controlled by another puppeteer. The central bank might seem like the one in charge but it's indirectly serving the government's wishes to print money out of thin air when they need it.

How they benefit: These groups benefit in various ways, creating a complex web of control. The government gets funds without immediate consequences, wealthy individuals and banks make money effortlessly, and the central bank keeps the show running. Meanwhile, the rest of the population might feel the effects, facing challenges as the system unfolds.

In the end, the fiat system's puppeteers create a show where a few benefit greatly but many are left wondering about the fairness of the financial stage they find themselves on.

The Role of Central Banks

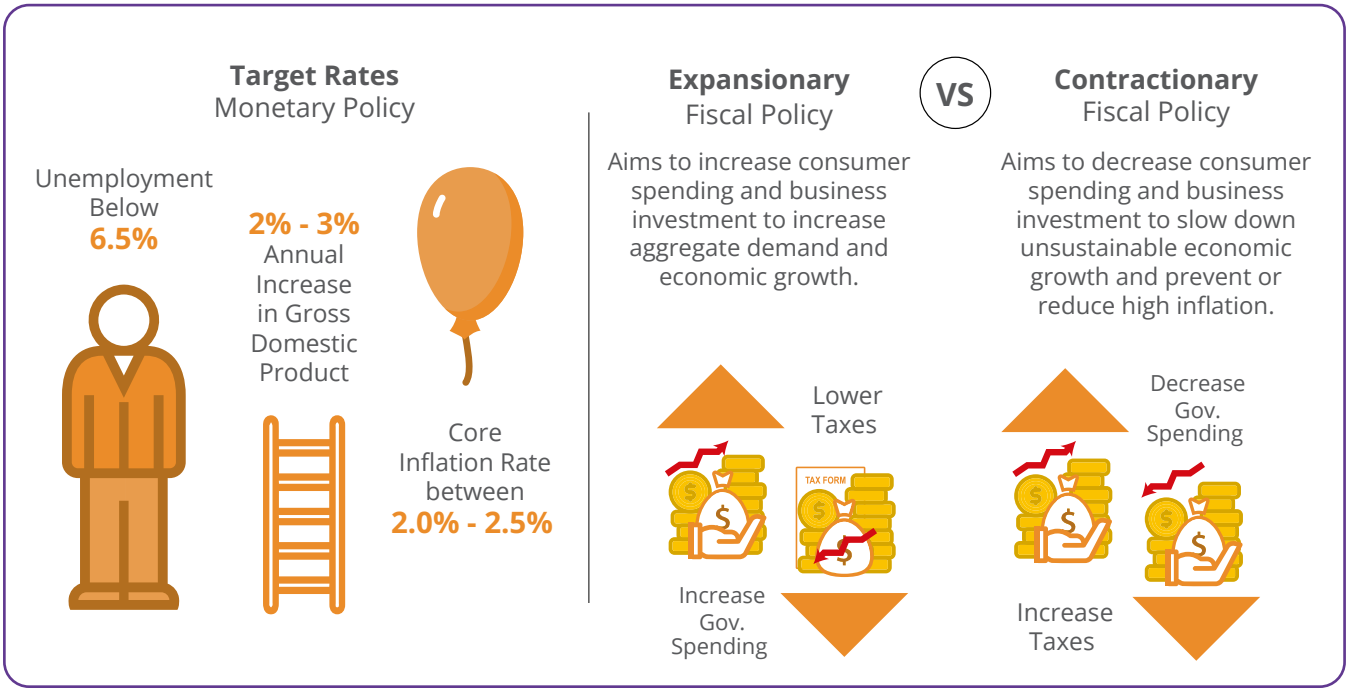
Central banks quietly shape how an economy works. Their official job is to ensure stability, integrity, and "keep things stable," but their methods reveal a more mysterious side.

Central banks work closely with governments and pull the strings of monetary policy, controlling the money supply with tools like interest rates. In times of crisis, they print money out of thin air and inject it into the economy through commercial banks, making it seem like everything is okay.

They don't just watch over things; central banks regulate commercial banks, set the rules of the game, and step in to help when banks are in trouble (acting as lenders of last resort). This web of control, while appearing protective, makes the economy and banks even more dependent on them.

Understanding where trillions of dollars in stimulus funds come from and who gets to decide how they are allocated is critical for comprehending the broader financial system. Governments use several tools to manage the money supply at specific moments in time.

Central banks and governments can use monetary and fiscal policy tools to influence the money supply and the economy. For example, the United States Federal Reserve (the Fed) uses monetary policy to adjust interest rates, affecting the amount of money in circulation. Fiscal policy, on the other hand, involves using spending and tax policies to influence economic activity.



Exchange rate policies, supply shocks, and price controls serve as additional tools to regulate the money supply and impact trade and the economy. While these policies aim to stabilize prices and control inflation, the intervention often leads to boom and bust cycles, creating challenges for everyone using the controlled currency.

Example: ”Too big to fail” refers to financial institutions so large and interconnected that their failure would have catastrophic repercussions for the entire financial system. During the 2008 financial crisis, several large banks were deemed “too big to fail,” leading the U.S. government to intervene and provide bailouts to prevent their collapse.

One of the most prominent examples of a “too big to fail” institution during the financial crisis was the investment bank Lehman Brothers. When Lehman Brothers filed for bankruptcy in September 2008, it set off a domino effect of events, including the near-collapse of insurance giant AIG and a massive drop in the stock market. The U.S. government had to intervene and provide bailouts to other major financial institutions to avert further chaos and safeguard the broader economy.

Knowing how these policies function is vital for understanding the limitations of centralized fiat monetary systems. Until you understand the problem, you won’t recognize the solution. Now that we’ve covered how the fiat system has worked in the past and present, we’ll discuss what the future of fiat currently looks like: Central Bank Digital Currencies, or CBDCs.

4.3 Central Bank Digital Currencies: The Future of Fiat Money

Central Bank Digital Currencies (CBDCs) are the next step of fiat currencies. Rather than a combination of physical bills, coins, and digital payments, CBDCs are fully digital forms of fiat currencies issued by governments and controlled by central banks.

Imagine the currency you use every day but without any physical presence — no coins to jingle in your pocket or bills to fold. What sets CBDCs apart is the heightened level of control and monitoring they offer to governments and central banks. With CBDCs, authorities gain unprecedented visibility into financial transactions, making it easier to track and regulate the flow of money.

Governments and central banks can readily adjust the form and supply of CBDCs, manipulate interest rates, and deploy monetary and fiscal policy tools with greater precision. In essence, CBDCs provide a more efficient means for authorities to influence and manage their fiat currency.

While CBDCs seem to be the future of fiat money, the world's current monetary system already operates on a pure fiat standard. Fiat currencies are no longer tied to gold, resulting in a significant expansion of the monetary supply without any real restriction.

Now that you have a clearer understanding of how the fiat system operates, it's time to explore its consequences in Chapter 5.

Chapter #5

How Problems Lead to Solutions

5.0 Introduction to the Problem

5.1 Decreasing Purchasing Power

- **5.1.1** Monetary Inflation and Its Effect on Purchasing Power
- **Activity:** The Effects of Inflation — An Auction Activity

5.2 The Global Debt Burden and Social Inequality

- **5.2.1** Impact on the Individual — Loss of Purchasing Power
- **5.2.2** Impact on Society — Increasing Wealth Inequality
- **Activity:** Consequences of the Fiat System
- **5.2.3** The Global Debt Burden

5.3 The Cypherpunks and the Quest for a Decentralized Currency

- **5.3.1** The Cypherpunks
- **5.3.2** Centralized vs. Decentralized Systems
- **5.3.3** Brief History of Digital Currencies

Student Workbook

English Version | 2025

How Problems Lead to Solutions

5.0 Introduction to the Problem

> Whoever controls the volume of money in our country is absolute master of all industry and commerce.. when you realize that the entire system is very easily controlled, one way or another, by a few powerful men at the top, you will not have to be told how periods of inflation and depression originate.
>
> **James A. Garfield, US President**

In Chapter 4, you learned that the financial world relies on a system that might not be as strong as it seems. The fiat system, held up by constant additions of paper money, seems to benefit a few more than many. This chapter uncovers what the fiat system means for regular people and society. Finally, we explore the story of a group of individuals who noticed these problems and quietly worked to find a solution that could change the future of human society.

5.1 Decreasing Purchasing Power

5.1.1 Monetary Inflation and Its Effect on Purchasing Power

Monetary inflation is the increase in the money supply within an economy, directly impacting the average person by reducing their purchasing power. The cycle of price inflation starts when there's more money in circulation. This, in turn, boosts the demand for goods and services, ultimately causing prices to go up.

Let's imagine a small group of friends — Alex, Bob, and Charlie — each with a dollar in hand, and there's one bottle of water available for sale. The initial situation is simple: three people with a total of three dollars and one bottle of water. Now, suppose someone — let's say the local government — decides to give each friend an extra dollar. Now, they collectively have six dollars. With this newfound money, they all feel like buying that single bottle of water. As all three friends want the same bottle, they start bidding against each other.

The increased demand, fueled by the extra money, prompts them to offer more than the initial price for the water bottle. In the end, the bidding war causes the price of the water bottle to go up. This situation reflects a decline in their purchasing power. Even though they have more money, they can't buy as many bottles of water as they could before, showcasing the impact of inflation on the value of their money.

In this example, the friends experienced a decrease in their purchasing power because they were using a form of money that was influenced by external factors, such as the additional dollars introduced by the government. The lack of control over the money supply, combined with increased demand, led to a rise in prices, making it more challenging for the friends to buy the same amount of goods with their extra dollars.

This illustrates how the friends' purchasing power was impacted by factors beyond their control, emphasizing the importance of understanding and questioning the systems that influence the value of our money.

Now, let's explore how this plays out in real life.

Activity: The Effects of Inflation — An Auction Activity

Objective: To understand the concept of inflation and how it affects the prices of goods and services in an economy.

Definitions:

- The Money Supply: the total amount of money in circulation within an economy at a specific time. This includes:
  - Physical currency, such as coins and bills
  - Checking accounts
  - Savings accounts
  - Money market accounts
  - Small time deposits (like certificates of deposit) under $100,000
- Auction: A public sale in which goods or property are sold to the highest bidder.

Class Exercise — Follow the Instructions Below:

1. You will receive a random amount of Monopoly money from the teacher. This represents the money supply in a society.
2. Write down the total money supply in the chart provided.
3. The teacher will auction a candy bar to the students. To win the candy bar, you will need to make the highest bid using your Monopoly money. Record the winning bid next to the money supply.
4. The teacher will then add a significant amount of Monopoly money to the total money supply. This represents an increase in the money supply in an economy. Later, you will learn how the money supply is increased or reduced in an economy.

Societies can often be unpredictable and unjust, exemplified by the simulation of a teacher randomly giving a significant amount of money to only a select few students. This mimics real-life situations where unequal distribution of resources and opportunities can occur, highlighting the inherent randomness and unfairness in many situations.

5. The teacher will auction a second candy bar to the students using the same process as before. Record the winning bid next to the money supply on the chart.
6. The teacher will repeat the auction a third time.

Round	Money Supply	Winning Bid
1		
2		
3		

Conclusion:

1. How did the increase in the money supply affect the winning bids for the candy bars?
2. What is the relationship between an increasing money supply and inflation?
3. How is the money supply relevant in the real world?
4. When new money is injected into the economy, what do you think will happen to the prices of goods and services? Do you think the changes in prices are temporary or permanent, and why? How do you think price changes affect citizens long-term?

5.2 The Global Debt Burden and Social Inequality

5.2.1 Impact on Individuals — Loss of Purchasing Power

Jaime is a college student who lives in a small apartment. He works part-time at a coffee shop to pay for his living expenses and tuition. As soon as he began living independently, Jaime became good at managing his own ledger.

A **ledger** is a detailed record of all of your monetary transactions. Whether it's money you're earning or spending, a ledger helps you keep track of it all.

At the beginning of 2023, he budgeted $10,000 for his living expenses for the entire year, including rent, food, and other necessities. These were his transactions for January 2023:

Date	Description	Amount	Type	Balance
01/01/2023	Starting Balance			**$1,600**
01/01/2023	Rent for January	**$800**	**Debit**	**$800**
01/05/2023	Groceries	**$100**	**Debit**	**$700**
01/15/2023	Part-time paycheck	**$500**	**Credit**	**$1,200**
01/20/2023	Gas for car	**$350**	**Debit**	**$850**
01/30/2023	Textbooks	**$150**	**Debit**	**$700**

This ledger shows that Jaime's starting balance was $1,600 out of which he spent (a debit) $800 to pay rent for the month. He then spent $100 on groceries and received $500 (a credit) in pay for his part-time job, bringing his balance to $1200. He then spent money on gas and textbooks, bringing his balance down to $700 at the end of the month.

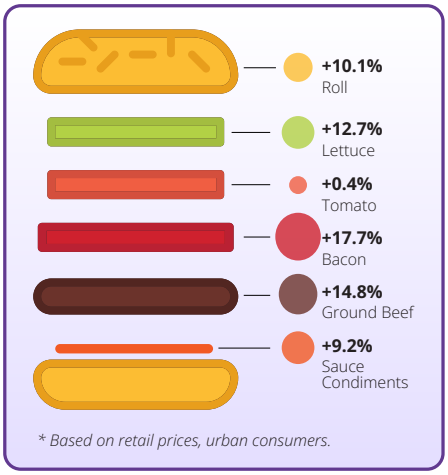
Twelve months later, Jaime is having lunch with his grandfather with whom he shares the details of his budget for 224. Jaime notices that his budget is not stretching as far as it used to and that his cost of living has increased significantly over the past year. While Jaime is wondering how this could be, his grandfather shows him the next image.

Jaime cannot believe his eyes. This is the moment he discovers that the cost of goods and services increase drastically over time, leading to a decrease in his purchasing power.

His grandfather says: *"In 1956, I was just a young man starting out in the world. I remember that I used to earn $380 a month as a factory worker. It may not seem like much, but it was a decent wage at the time. In fact, I was able to save up enough money to buy my own house in the suburbs."*

The grandfather continues: *"The costs of things were very different in the past century. For example, in 2020, purchasing 30 Hershey's chocolate bars would cost you $26.14. However, if we go back in time to 1913, the cost for the same number of Hershey's bars would only be $1.00."*

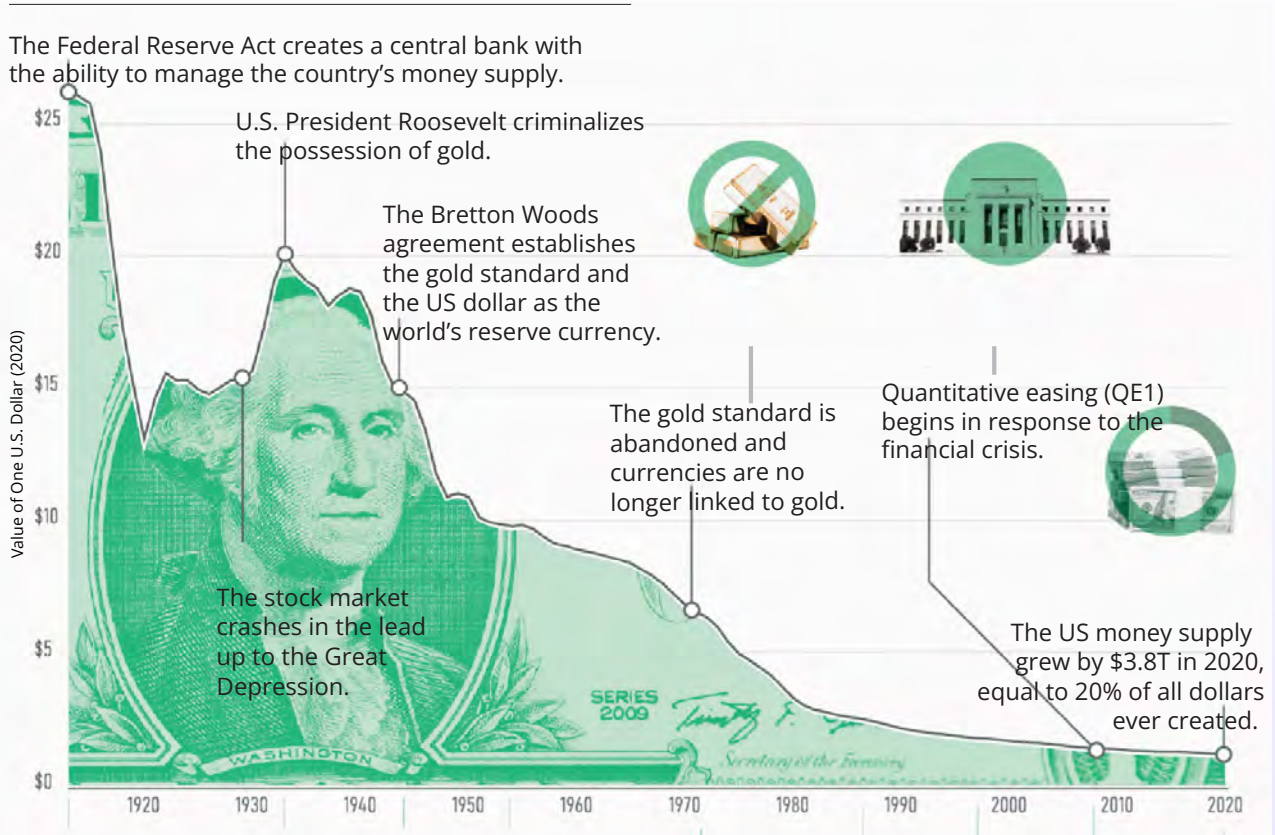
This significant difference in price highlights the change in purchasing power over time and how it has shifted over the years due to inflation.



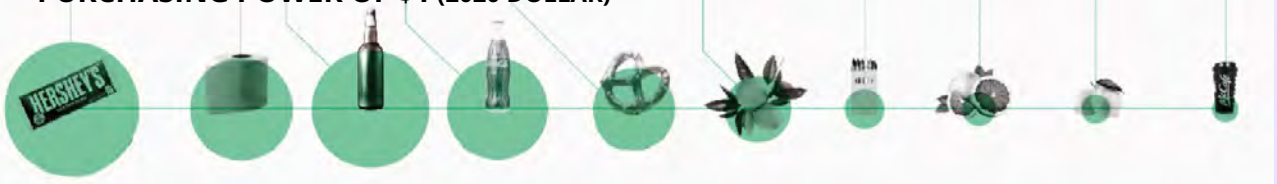
How Problems Lead to Solutions

A Dollar's Worth
Purchasing Power of the U.S. Dollar

The purchasing power of the US dollar has fallen sharply over the last century due to rising inflation and money supply.



PURCHASING POWER OF $1 (2020 DOLLAR)



$26.14	$15.14	$15.14	$14.71	$9.69	$6.39	$2.28	$1.61	$1.20	$1.00
30 Hershey's chocholate bars	10 rolls of toilet paper	10 bottles of beer	20 bottles of Coca-Cola	10 bags of pretzels	17 oranges	2 boxes of crayons	4 grape fruits	2 lemons	1 McDonald's coffee
1913	1929	1933	1944	1953	1971	1987	1997	2008	2020

Jaime: *"What? That's crazy. I can't imagine how low my rent would have been then compared to now."*

Grandfather: *"Well yes, your rent would have been much cheaper back then. I have another example to illustrate this: back then, $1 would have bought you about 10 bags of pretzels. In 2020, I paid $9.69 for the same amount. Imagine how much 10 bags of pretzels would cost today."*

Jaime: *"Wow, that's really interesting, Grandpa. How did you experience this yourself when you were younger?"*

Grandfather: *"Oh, Jaime, everything was just much cheaper when I was young. A loaf of bread would only cost $0.18, and you could buy a gallon of gasoline for just $0.29. It is unbelievable how much the cost of living has gone up."*

After the conversation with his grandfather, Jaime goes home to take another look at his ledger. He quickly discovers that he needs to budget an additional $1,000 for 2024 to be able to buy the same basket of goods and services that he purchased in the previous year. This means that his purchasing power has decreased by $1,000 as he now has to spend more money to buy the same goods and services. While Jaime's salary only increases minorly, his cost of living skyrockets every year.

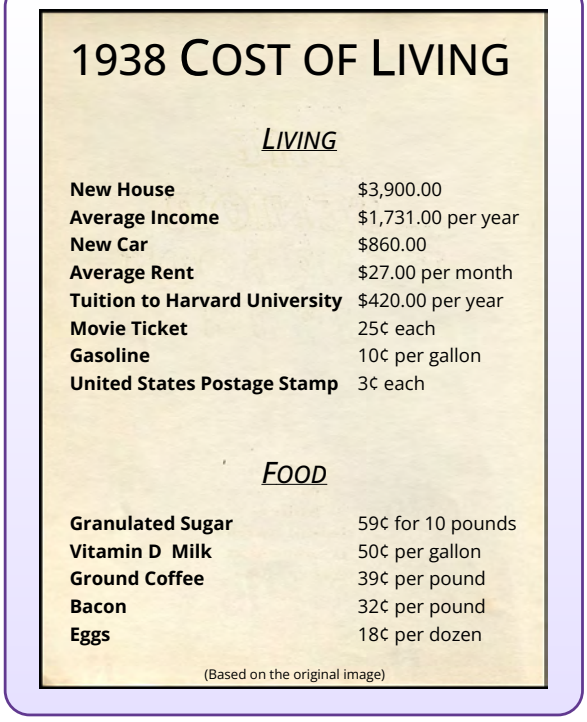
The following table shows Jaime's costs in the first and second years, as well as the percentage increase in price.

In order for Jaime to live under the same standard of living, he will need to work more hours per week to receive an additional $1,000.

Based on information from the US Bureau of Labor Statistics, prices today are about 30 times higher than they were in 1913. This means that a dollar today can buy only around 3% of what it could buy back then.

Item	Cost Year #1	Cost Year #2	% Increase
Rent	$4,000	$4,500	12.5%
Groceries	$2,000	$2,300	15%
Necessities	$4,000	$4,200	5%
Total	**$10,000**	**$11,000**	**10%**

To illustrate, someone offering Jaime a time-travel choice — either take $100 in 1913 or wait until 2023 and receive only $3 — is like choosing between a past shopping spree or getting just a few small treats today. The significant difference in value shows how much money's purchasing power has decreased over the years.



1938 COST OF LIVING

LIVING

New House	$3,900.00
Average Income	$1,731.00 per year
New Car	$860.00
Average Rent	$27.00 per month
Tuition to Harvard University	$420.00 per year
Movie Ticket	25¢ each
Gasoline	10¢ per gallon
United States Postage Stamp	3¢ each

FOOD

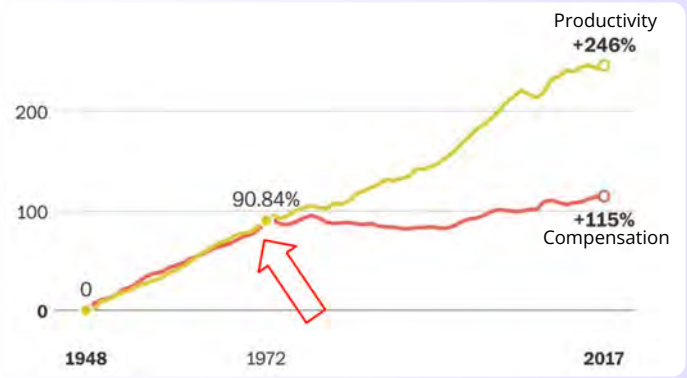
Granulated Sugar	59¢ for 10 pounds
Vitamin D Milk	50¢ per gallon
Ground Coffee	39¢ per pound
Bacon	32¢ per pound
Eggs	18¢ per dozen

(Based on the original image)

How Problems Lead to Solutions

When we think in numbers, Jaime earns many more dollars in a year than his grandfather ever did, but the dollars that Jaime's grandfather possessed were much more valuable and could buy much more back then.

Growth in Productivity and Hourly Compensation 1948 — 2017



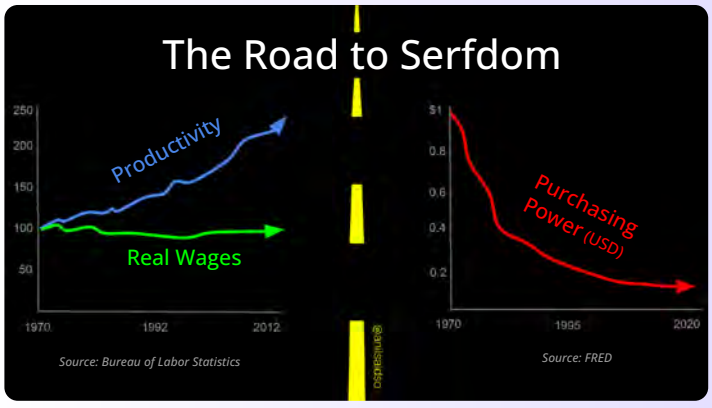
NOTE: Compensation includes wages and benefits for production and non-supervisory workers.

In today's world, the significant impact of inflation discourages people from saving money.

Instead, most choose to spend their money immediately because its value decreases rapidly. This pessimistic outlook hampers their ability to plan for the future.

As seen in the graph, the average individual's salary growth remains stagnant when adjusted for inflation, meaning they aren't receiving raises at the same rate as the decreasing value of their money, despite working harder.

Jaime's example is just one among many. In the fiat world, it's quite common for governments to create money out of thin air to further their own agenda, leaving individuals worldwide to bear the consequences. The prices of everyday items, from bread to housing, and from groceries to holidays, increase each year. While the rich benefit from inflation due to owning assets, ordinary folks see their hard-earned money lose its value. The result? People and families worldwide struggle due to the decrease in their purchasing power.



People around the world find themselves working more jobs and longer hours just to maintain the same standard of living. It's like being on a treadmill — running faster and faster but never really getting ahead. The fiat system leaves individuals feeling like they are in a perpetual race against rising prices.

In their struggle to keep pace with increasing costs, many turn to credit, which is like using a small Band-Aid on a very deep wound. People take on loans or make impulsive decisions just to get by. Fast money becomes a necessity, and individuals find themselves in a cycle where survival today takes precedence over planning for tomorrow.

The fiat system, with its constant money printing, impacts humanity's psychology. It instills a high time-preference — a focus on short-term gains over long-term planning. Just like a quick fix for immediate relief, individuals in the fiat world tend to prioritize short-term benefits. It is a survival instinct, creating a cycle of dependency where individuals seek any means to obtain fast money, even if it is not sustainable or workable in the long run.

In essence, the impact of the fiat system paints a challenging picture for individuals globally. In the fiat system, prices rise, incomes stagnate, and the struggle to survive becomes a daily battle. While certain groups get richer, most individuals worldwide stay dependent on a system that makes them poorer and poorer.

5.2.2 Impact on Society — Increasing Wealth Inequality

In a society based on sound money, a government's financial decision-making is tied to the people's approval. However, in the fiat system, governments can go into unlimited debt on the backs of their citizens.

The power to print money at will often leads to political centralization. The fiat system enables governments to accumulate massive debts, making decisions that benefit themselves rather than the majority. Superpowers like the United States gain a competitive edge due to this phenomenon. They can print money endlessly to fund their plans, including wars. This ability allows these dominant nations to control, influence, and engage in geopolitical conflicts, creating a global power imbalance. Wars and major actions to control others become financially feasible for superpowers while others without the same financial flexibility face limitations.

Under the fiat system, wealth does not distribute itself evenly. Instead, it tends to concentrate in the hands of a select few. This phenomenon is like playing a game of Monopoly where a handful of players possess almost all the hotels and properties while the majority struggle to stay afloat. The fiat system has become a tool for certain groups to concentrate wealth. Money printing allows governments and their tight collaboration with central banks to inject more currency into the economy, and the recipients of this newly created money are those with existing wealth and status — powerful entities and individuals. These groups benefit from the freshly printed money before its negative effects, like a decrease in purchasing power, start to manifest through the economy.

How Problems Lead to Solutions

Wealth inequality is not just about the haves and have-nots; it is about suppressing economic mobility. Those from less privileged backgrounds find it increasingly challenging to climb the economic ladder, akin to starting a race with a heavy backpack. The growing gap between the rich and the poor causes problems for everyone, with the wealthy shaping policies in their favor. This makes things harder for regular people, leading to social unrest, a lack of trust in institutions, and communities falling apart like a house of cards. The fiat system's instability manifests in economic uncertainty, political unrest, and global repercussions when the Western world faces an economic downturn.

This is a global phenomenon, affecting societies in developed and developing nations alike. Sometimes, wealthy individuals and groups take this opportunity to use the global financial system to their advantage, which can further widen the gap between the upper and lower classes.

Under the fiat system, getting into debt has become the norm for humanity. Governments, institutions, businesses, and individuals worldwide find themselves immersed in a sea of debt.

The psychological shift toward considering debt acceptable has its roots in the fiat system's design. During the past several decades, it has become easier and easier for entities to take on substantial debt, and it often becomes a necessity for ordinary people due to rising prices and living cost of living.

Consumerism, a constant urge to buy and consume, leads people to purchase more than they need, resulting in overconsumption and waste. While it may seem like a never-ending shopping spree, the real cost goes beyond the price tag, impacting people's psychological health and well-being.

It becomes clear that the fiat system is not just an economic mechanism. Rather, it is a system that shapes human society as a whole. From the concentration of power to global dynamics, wealth disparities, and societal norms, the fiat system directly influences how nations operate and how regular citizens navigate their lives.

Activity: Consequences of the Fiat System

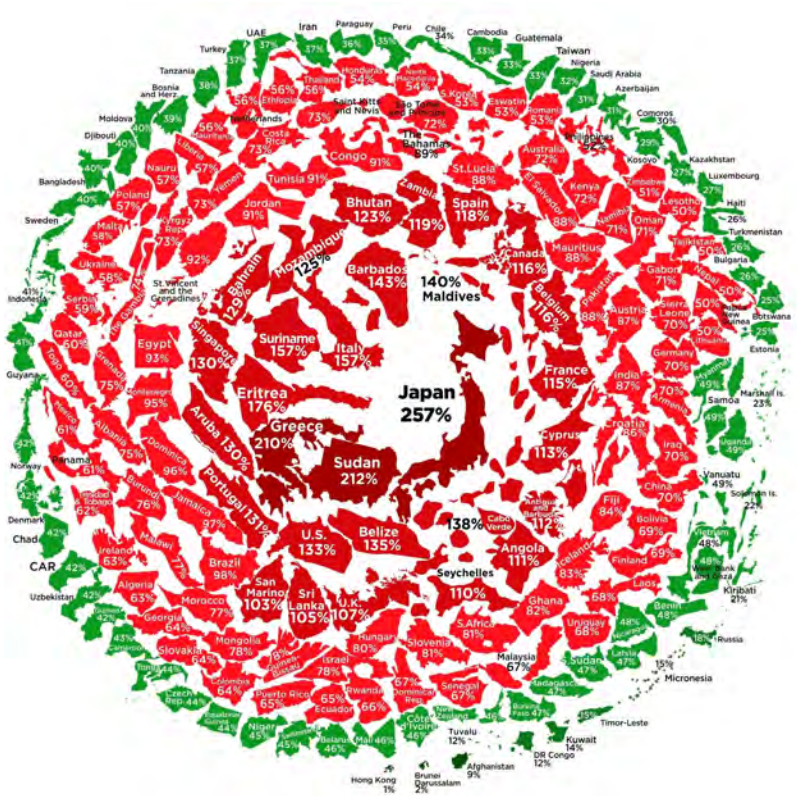
1. Are there any other consequences that individuals and society as a whole experience as a result of the fiat system?
2. What are the consequences of the fiat system in your country? What has happened throughout history, and how did that affect the people in your country?
   a. Personal examples: interactive session

5.2.3 The Global Debt Burden

As a result of the fiat system, governments across the globe find themselves stuck in an enormous web of debt, caught up in what is called, "The global debt spiral." Imagine a scenario where you borrow more money than you can ever hope to repay. This is happening on a massive scale worldwide. Governments, drowning in debt, have been caught in a dangerous game of accumulating more debt than they can ever pay back. It's a story of reckless spending, borrowing, and a lack of foresight that now pushes nations around the world to the brink of financial disaster.

As of today, the U.S. federal government has added a staggering $1 trillion of new debt since 219. Total debt has skyrocketed from about $23 trillion during the fourth quarter of 219 to an astronomical $34 trillion today. The pace at which governments globally churn out new debt isn't slowing down; in fact, it's accelerating. The year 223 was projected to be the most debt-additive year since the turbulent times of 2021, marked by the COVID pandemic.

The State of the World´s Government Debt



So, what does this mean for the individuals and societies that already need to deal with the consequences of the fiat system? The debt spiral they are caught up in is like a snowball rolling down a hill—it just keeps getting bigger, and we're not sure how to stop it.

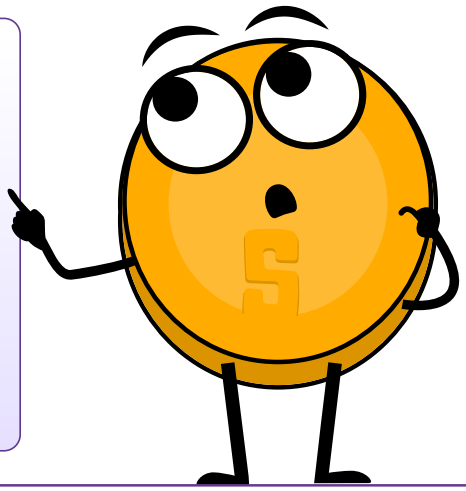
The consequences mentioned earlier, from wealth inequality to societal unrest, won't fade away. Instead, the global debt burden has reached a point of no return, ensuring that things are destined to get worse.

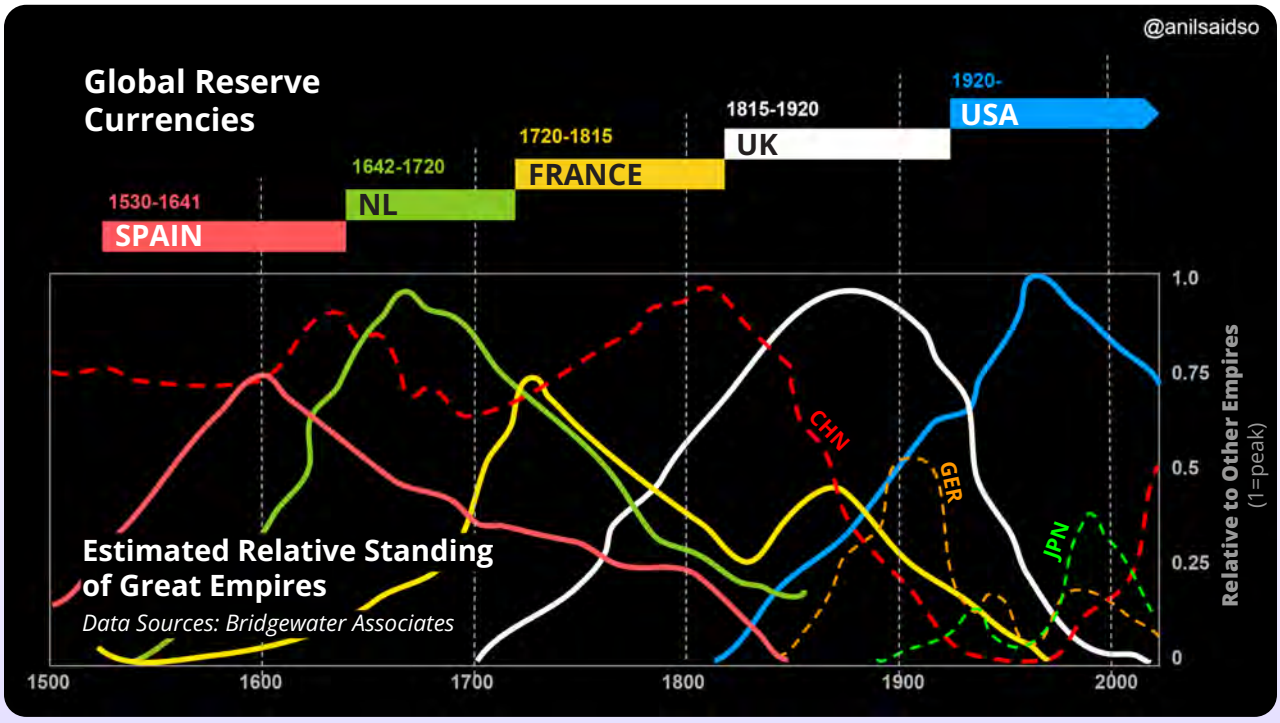
Debt to GDP Ratio 2021 (%)

- 200% or more
- 100% — 199.9%
- 50% — 99.9%
- 20% — 49.9%
- 10% — 19.9%
- Less than 10%

How Problems Lead to Solutions

> I don't believe we shall ever have good money again until we take the thing out of the hands of government... all we can do, is by some sly, roundabout way, introduce something that they can't stop.
>
> ***Friedrich Hayek***
> Nobel Prize Winner of Economics





5.3 The Cypherpunks and the Quest for a Decentralized Currency

We have observed the progressive capture of money by banks and governments throughout history, leading to the fiat system we know today and its disastrous consequences for society. But the rise of new technologies like encryption and the internet have allowed new ideas to emerge, such as independent digital money — free of government intervention, open and accessible to all. Let's dive into the journey of those leading this revolutionary movement: the Cypherpunks.

5.3.1 The Cypherpunks

> The computer can be used as a tool to liberate and protect people, rather than to control them.
>
> **Hal Finney**

The second half of the 20th century saw the rise of multiple technological breakthroughs, like the computer and the internet, paving the way for a new digital age.

A group of people discovered that these massive innovations would soon transform how society functions. They foresaw both the potential and the danger of the personal computer, either as a freedom-enabling tool to empower the individual or as a tool for complete control and surveillance.

These people were called the Cypherpunks. They emerged as a loosely connected group of activists, cryptographers, programmers, and privacy activists who shared a common vision: the pursuit of privacy, security, and a decentralized digital future. The term "Cypherpunk" is a fusion of "cypher," referring to cryptographic code, and "punk," representing the countercultural ethos of rebellion.

The Cypherpunks believed in cryptography's power to protect individual liberties. Their goals included developing tools to secure online communications, anonymize internet activities, and establish digital currencies to operate beyond the control of centralized authorities.

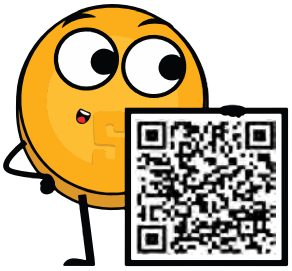
The Cypherpunks understood the consequences of the fiat system and saw the threat of an “Orwellian future.” They believed they had to ensure that the personal computer and the internet would become good things for humanity instead of tools that could exacerbate the state's control over its people.

THE DEFINITION OF AN ORWELLIAN FUTURE:

An Orwellian future refers to a dystopian vision inspired by George Orwell's works. The term is associated with a nightmarish and totalitarian society characterized by oppressive government control, extensive surveillance, propaganda, and the manipulation of information. The term "Orwellian" often describes a scenario where citizens' freedoms and individual autonomy are severely restricted, dissent is suppressed, and reality is distorted to serve the interests of a powerful and authoritarian regime. The concept is named after George Orwell, who, in his writings, warned against the potential dangers of unchecked government power and the erosion of fundamental human rights.

How Problems Lead to Solutions

Key figures within the Cypherpunk movement included luminaries like Eric Hughes, Timothy C. May, and John Gilmore. In 1992, Eric Hughes penned "A Cypherpunk Manifesto," outlining the group's principles. The manifesto emphasized the importance of privacy, encryption, and the need for individuals to take control of their digital identities.



Watch this video and discover the story of the Cypherpunks!

One of the Cypherpunks most notable inventions was the creation of cryptographic tools and protocols. In 1991, Phil Zimmermann introduced PGP (Pretty Good Privacy), email encryption software that became a flagship project. PGP allowed users to send encrypted messages over the internet without anyone except the intended recipient being able to decrypt them. Before that, any message sent over the internet could be intercepted and read by others, like governments.

The Cypherpunks thought that the breakthrough of encryption, along with the internet and the computer, provided a solid foundation for the creation of decentralized networks in the digital space, allowing individuals to communicate and transact on the internet privately and without interference from a central authority.

The Cypherpunks were on the right track to fostering a brighter future for humanity, where technology would be a tool to maximize freedom instead of control. The only missing pieces were a decentralized network and a digital currency.

5.3.2 Centralized vs. Decentralized Systems

Centralized Systems: One Ruler, Many Problems

In a centralized system, everything revolves around one main authority, like a tall building in a city. This authority controls how the entire system works. Think of traditional banks as an example, where a small group makes all the decisions.

Real-world example: In 2022, during peaceful protests in Canada, banks froze protestors' accounts, showing how a central authority could step in and control financial access.

Problems with Centralized Systems:

- Central point of failure: If something goes wrong with the central authority, the whole system can collapse.
- Control: A small group at the top has all the control and power, often making decisions that benefit them more than everyone else.
- Inefficiency and intermediaries: Like traffic jams in a city, centralized systems can become slow and expensive because of unnecessary middlemen.
- Lack of autonomy: People might not get to make their own financial choices; it's all decided by the top authority.
- Censorship and restriction: Just like some parts of a city can be blocked off, centralized systems may block or limit access to certain financial resources.
- Scaling challenges: When more people need financial services, centralized systems may struggle to keep up.
- Security risks: Problems with the central authority can put the whole system at risk of cyberattacks.
- Lack of transparency and trust: The inner workings of centralized systems can be hard to understand, making it tough for people to trust them.

Decentralized Systems: Power to the People

Now, think of a decentralized system like a big forest. Each tree represents a separate part, and the whole forest represents the entire system. Unlike a city with a single central point, a decentralized system is more like a resilient forest that can keep going even if one part faces problems.

- Real-world example: The Tor network and its browser create a decentralized system where people can stay anonymous on the internet and the network is difficult to stop or censor.

Benefits of Decentralized Systems:

- Enhanced resilience and reliability: There is no single point of failure, which makes the system strong, even if there are some issues.
- Increased security: With the right encryption/protection, a decentralized system is better at resisting control from a single authority.

How Problems Lead to Solutions

- Greater sovereignty: People have more control over their money, data, and decisions.
- Improved transparency: Everyone sees the same information, making the system more trustworthy.
- Permissionless and limitless nature: Anyone can join or take part, making it an inclusive financial system.
- Equal opportunities: Everyone has a fair chance to contribute and have a say.
- Enhanced privacy: Data is distributed across multiple participants and mostly pseudonymous, making decentralized systems more private.

While decentralized systems have lots of advantages, making decisions together can be a bit tricky. It requires everyone to work together.

Changing How Power is Wielded

In a world of centralized and decentralized systems, it's all about who holds the power. Centralized systems give power to a small group, while decentralized systems spread it out, letting everyone have a say. This shift in power would mean a fairer and more democratic future, where many people influence the system that shapes their lives.

5.3.3 Brief History of Digital Currencies

One of the most pivotal concepts discussed by the Cypherpunks was digital cash. The Cypherpunks realized that the state and money needed to be separate to ensure that the future would benefit the common good. David Chaum's groundbreaking work on cryptographic protocols for secure and private transactions laid the groundwork. The downside was that this protocol required a central authority to function efficiently, raising concerns about a single point of failure and potential censorship.

In the years that followed, multiple Cypherpunks attempted to iterate each other's ideas to create a workable solution for a digital currency free from government control. The table below describes several key innovations the Cypherpunks developed in their quest to create digital cash:

Name and Date	Description	Limitations
E-Cash (1982)	David Chaum's E-Cash was an early concept of electronic cash, focusing on privacy through cryptographic techniques.	Required a central authority, raising concerns about a single point of failure and potential censorship.
DigiCash (1990)	DigiCash, founded by David Chaum, aimed to create a digital form of currency with an emphasis on privacy.	The centralized model contributed to its eventual bankruptcy in 1998.

B-money (1996)	B-money, proposed by Wei Dai, was a theoretical proposal for an anonymous, distributed electronic cash system.	Lacked a practical implementation; remained a conceptual idea.
Hashcash (1998)	Hashcash, developed by Adam Back, was a proof-of-work system designed to limit email spam and denial-of-service attacks.	Did not directly address the double-spending problem associated with digital currencies.
Bit Gold (1998)	Bit Gold, proposed by Nick Szabo, described a decentralized digital currency system with elements of proof-of-work.	Never implemented, remained a theoretical concept.
e-Gold (2004)	e-Gold was a centralized digital currency backed by physical gold, allowing users to buy and transfer e-Gold units.	Legal issues led to its closure in 2009, highlighting challenges associated with centralized digital currencies.

Despite the Cypherpunks' numerous attempts made over the decades to create a digital currency free from the control of any one group or government, their efforts faced practical challenges and couldn't fully materialize in the real world. The Cypherpunks concluded that it was not easy to build a digital form of cash that was secure, scalable, and had the potential to become widely adopted.

However, the story takes a turn when one individual, learning from the Cypherpunks' lessons elevated the concept of a decentralized digital currency to new heights. In the following chapters, we'll explore how this person's contribution, building upon 40 years of prior work, ultimately led to the creation of a functional system.

Chapter #6

An Introduction to Bitcoin

6.0 Satoshi Nakamoto and the Creation of Bitcoin

6.1 How Does Bitcoin Work?

- **6.1.1** The Nakamoto Consensus Mechanism
- **6.1.2** The Players of the Game
- **Activity:** Consensus Building in a Peer-to-Peer Network

6.2 Bitcoin as Sound Digital Money

- **6.2.1** Introduction
- **6.2.2** Bitcoin's Features
- **Activity:** Class Discussion - Is Bitcoin Sound Money?
- **6.2.3** Embracing Personal Responsibility

Student Workbook

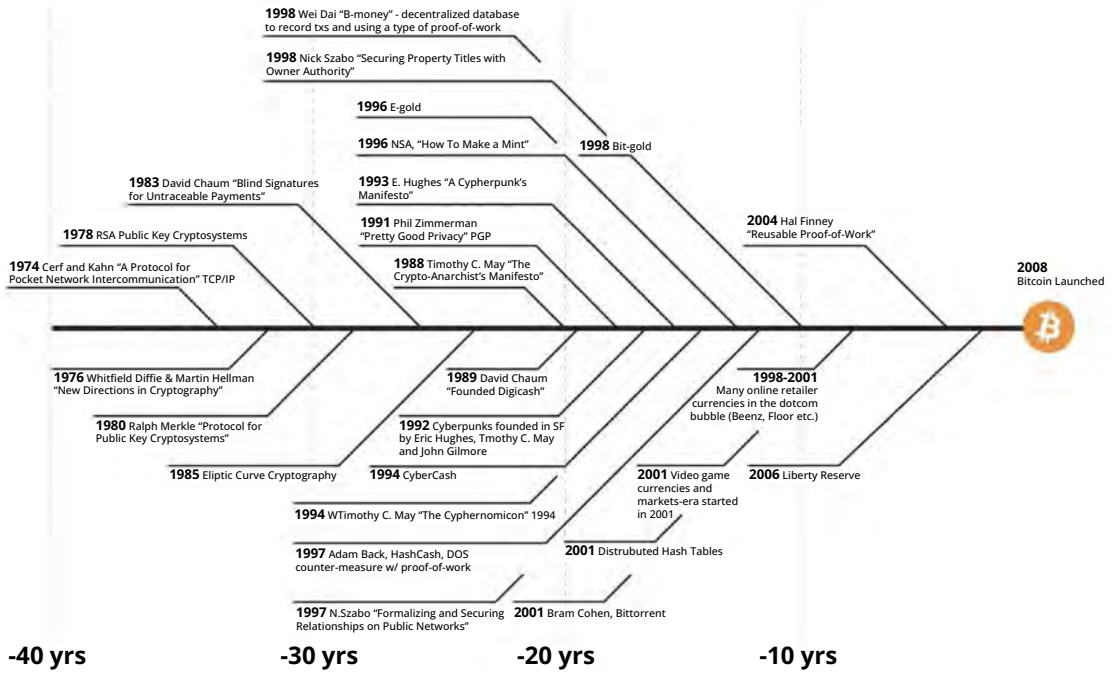
English Version | 2025

An Introduction to Bitcoin

6.0 Satoshi Nakamoto and the Creation of Bitcoin

> A lot of people automatically dismiss e-currency as a lost cause because of all the companies that failed since the 1990s. I hope it's obvious it was only the centrally controlled nature of those systems that doomed them. I think this is the first time we're trying a decentralized non-trust-based system.
>
> **Satoshi Nakamoto**

Bitcoin prehistory: — It's the result of 40 years of research, development and demand



As you read in the previous chapter, multiple Cypherpunks attempted to create an alternative money system. This chapter continues the story of one of them: a visionary mind by the name of "Satoshi Nakamoto." This anonymous person (man, woman, or group), long before Bitcoin, was one of the cryptography enthusiasts like computer scientists and hackers, engaging in discussions to find practical solutions to replace the fiat system.


Page: [1] « previous topic next topic » print

Author | Topic: Added some DoS limits, removed safe mode (0.3.19) (Read 25115 times)

satoshi (OP)
Founder
Sr. Member

Activity: 364
Merit: 6671

Ignore

Added some DoS limits, removed safe mode (0.3.19)
December 12, 2010, 06:22:33 PM

There's more work to do on DoS, but I'm doing a quick build of what I have so far in case it's needed, before venturing into more complex ideas. The build for this is version 0.3.19.

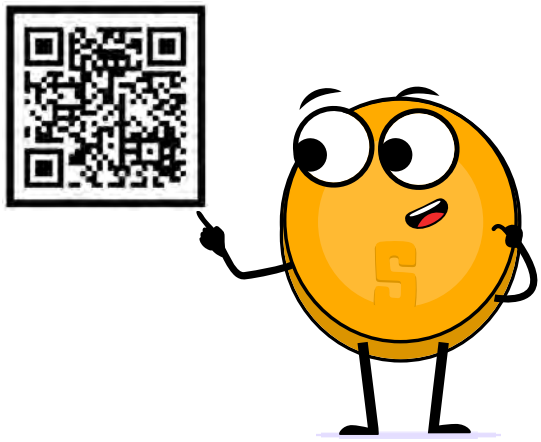
- Added some DoS controls
As Gavin and I have said clearly before, the software is not at all resistant to DoS attack. This is one improvement, but there are still more ways to attack than I can count.

I'm leaving the -limitfreerelay part as a switch for now and it's there if you need it.

- Removed "safe mode" alerts
"safe mode" alerts was a temporary measure after the 0.3.9 overflow bug. We can say all we want that users can just run with "-disablesafemode", but it's better just not to have it for the sake of appearances. It was never intended as a long term feature. Safe mode can still be triggered by seeing a longer (greater total PoW) invalid block chain.

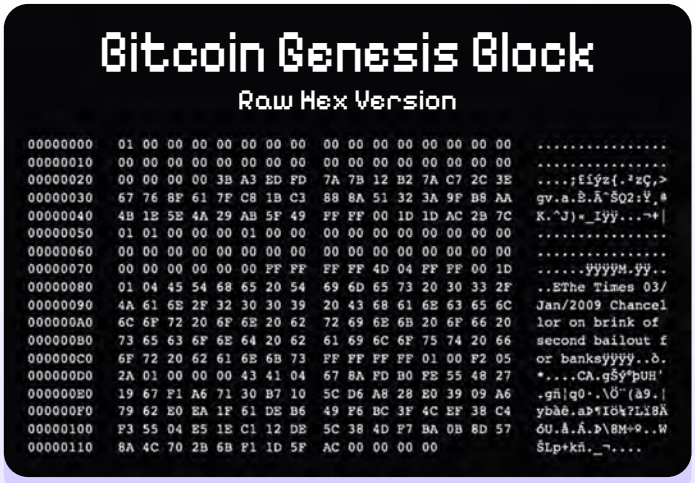
Builds:
http://sourceforge.net/projects/bitcoin/files/Bitcoin/bitcoin-0.3.19/

In October 2008, Nakamoto unveiled a groundbreaking whitepaper titled, “Bitcoin: A Peer-to-Peer Electronic Cash System” on a cryptography mailing list. This document laid the foundation for a decentralized peer-to-peer protocol, designed to facilitate secure online transactions without the need for intermediaries.



Nakamoto's vision was clear: to create a purely peer-to-peer version of electronic cash, free from the control of powerful governments and financial institutions.

Fast forward to January 3, 2009, when Nakamoto mined the first Bitcoin block known as the "genesis block." This marked the official launch of the Bitcoin network, a new money system built on trust and security through a decentralized ledger. In the months and years that followed, more and more enthusiasts started to join and contribute to the idea.



In 2011, after the Bitcoin network proved it could operate successfully without the need of its influential creator, Nakamoto sent an email to a fellow Bitcoin developer, announcing they were removing themselves from the Bitcoin scene and giving its future away to other “good hands” that shared their vision.

Although Nakamoto’s identity remains a mystery until this very day, their goal for creating Bitcoin was never a mystery. In essence, Nakamoto created it to take the power away from the few and give it back to the many by creating an alternative in the form of a decentralized, open-source, transparent money system, separating money from the state. Creating Bitcoin was Nakamoto’s response to the 2008 financial crisis that hurt regular people worldwide while enriching the elite class — again. Bitcoin was Nakamoto’s answer to the corruption and fragility of the fiat system. Nakamoto set the foundation for a new revolution and walked away from it instead of claiming credit.

In the years that followed, Bitcoin started to grow quickly and emerged as a symbol of hope, empowerment, and resilience, challenging the fiat system and providing a secure, censorship-resistant means of financial transactions. Bitcoin is an open-source protocol, meaning that no one has the power to own or control it. Its design is public and open for anyone to participate.

Today, Nakamoto's dream of a borderless, transparent, and secure financial system lives on, empowering the global freedom revolution we are witnessing today. Every day, ordinary people are opting out of the fiat system and into the world of Bitcoin. Bitcoin hubs — the so-called Bitcoin circular economies — have been launched by freedom enthusiasts in regions all over the world. Even entire countries looking for an alternative path, like El Salvador, are starting to adopt Bitcoin in their own ways.

6.1 How Does Bitcoin Work?

6.1.1 The Nakamoto Consensus Mechanism

So, how does Bitcoin work? Bitcoin has lots of features, and the rabbit hole goes deep — very deep. Fortunately, if you enter the Bitcoin world for the first time, you do not have to perfectly understand how it works to start using it.

The same counts for using the internet: most people do not know how the TCP/IP protocol works, yet they send emails and, messages, and post content on their social media accounts every day. The same goes for driving a car — most people do not know exactly how a car works, yet they do know how to drive.

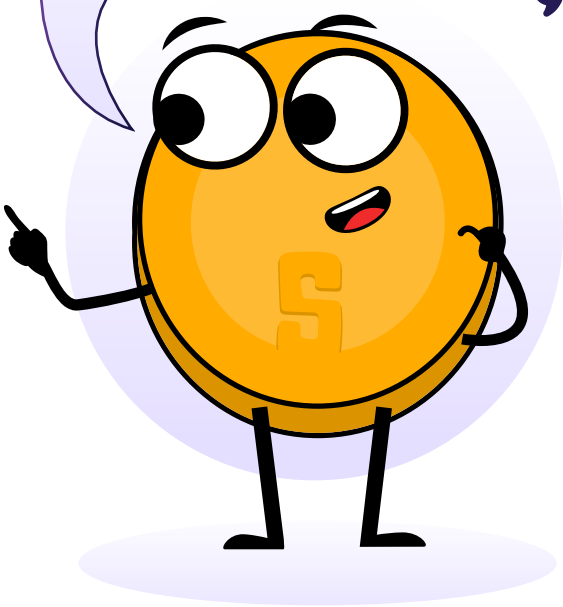
However, Bitcoin is not yet widely adopted. It is still a pretty new technology, like the internet was during the 90s. Because of this, it can be helpful to grasp the basics of Bitcoin in a simple, less technical way.

The key idea behind how Bitcoin operates can be condensed into one sentence: Bitcoin is an agreement among people online. You can think about it like playing a board game with friends. With a game like Monopoly, you are in agreement with the other players about specific rules. One of the rules of Monopoly is that only special “Monopoly bills” are to be accepted. If James, (one of the players), went against the rules by using toilet paper to buy a house instead of Monopoly bills, the other players would tell James he is a cheater and would simply stop playing with him. In short, to play the game, you have a consensus on a set of rules with each other and you do not drift away from those rules, otherwise you will be rejected.

This is essentially how Bitcoin works. Bitcoin is a network of people that agree on the same set of rules. These rules are mathematically bound, written in computer code, and accepted directly by everyone who runs the Bitcoin software. The rules of Bitcoin apply to all participants equally, which means that everyone either follows the rules of the game or cannot play because the network will reject them.

For example, one of the rules of Bitcoin is, "There will never be more than 21 million bitcoins." If someone wanted to create a million extra bitcoins for themselves, it would be of no use to them because they would automatically be identified and rejected by everyone else. This is what makes Bitcoin so robust.

> Did you know that, since 2009, Bitcoin has withstood tens of thousands of attempts to hack, tamper with, or alter it? Bitcoin has proven that nobody can stop, control, or manipulate it.



It does not matter who you are or where you come from; if you enter the Bitcoin world, you need to play by the same set of rules as everyone else.

This also applies to all the people and entities with an enormous amount of control and influence in the fiat world. In the Bitcoin world, there is no room for cheating or sabotage — everyone is treated equally, and no one can change that.

6.1.2 The Players of the Game

To better understand the decentralization of Bitcoin, we need to dive deeper into the different roles within the network. In the Bitcoin world, various participants play distinct yet harmonious roles, contributing to the network's seamless functioning.

1. Miners: The Architects of Security

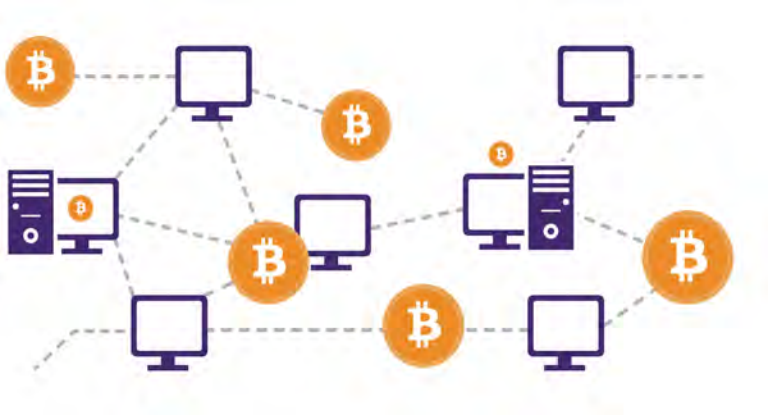
Miners are the backbone of Bitcoin. These are people or groups of people who work behind the scenes to maintain and secure the network through a mechanism called Proof-of-Work (PoW). These players are armed with special computers that have heavy computational power. They make their hardware available to the Bitcoin network, competing with each other in a worldwide lottery to add new blocks of transactions to Bitcoin's decentralized ledger (the blockchain). Their commitment ensures the the ledger's immutability and guards against malicious attacks.

Mining's decentralized nature allows anyone with sufficient computing resources to participate. Because of their hard work, the miners who solve the puzzle the quickest are rewarded in the form of bitcoins.

Bitcoin miners are distributed all over the world, safeguarding the network against centralization and ensuring Bitcoin's security stays robust and distributed.

2. Nodes: Gatekeepers of Validation

Bitcoin nodes are ordinary people who live across the planet. These participants serve as the Bitcoin network's gatekeepers by running Bitcoin software on their small computers on which they maintain a copy of the entire ledger. Nodes validate transactions and ensure that all participants adhere to the consensus rules.



By distributing the responsibility of validation across a network of nodes, Bitcoin remains resilient against attacks and maintains its trustless nature. Nodes play a crucial role in upholding the integrity of the ledger, contributing to the Bitcoin's decentralization ethos.

3. Users: Empowered Participants

Users — the lifeblood of the Bitcoin network — are individuals who engage in transactions. You can think of users as regular people who just live their lives but have also empowered themselves by integrating Bitcoin. For example, some users save their money in bitcoins while others, like citizens of El Salvador, use it as money to buy groceries and receive their salary in bitcoin.

Bitcoin empowers users by eliminating the need for intermediaries like banks and governments, allowing for direct peer-to-peer transactions. This also means that users have full control over their money, and transactions.

4. Developers and Projects: Architects of Innovation

The monetary system of the future won't build itself on its own, nor will it be globally adopted in an ethically correct way without effort. That’s where Bitcoin developers and projects come into play.

Developers wield their technical expertise to enhance and innovate the Bitcoin protocol. These individuals contribute code, propose improvements, and address vulnerabilities, ensuring the network evolves in response to all types of challenges. Bitcoin's open-source nature invites collaboration, allowing developers worldwide to contribute to its growth.

The beauty of this decentralized development prevents a single entity from monopolizing control over the protocol. This happens through a consensus-driven process. Developers propose ideas and changes, and only those with the best ideas who are aligned with the broader vision for a better world receive support from the community, empowering Bitcoin's transparent and democratic evolution until it’s ready for 8 billion people.

Bitcoin projects involve diverse groups, from mission-driven nonprofits and corporations to groups and individuals that create valuable content. These people work together on a specific goal or focus within the bigger Bitcoin mission toward collective freedom.

Bitcoin projects play a crucial role in shaping and promoting the adoption of Bitcoin, working toward a future that prioritizes the empowerment and freedom of the human race.

The Symphony

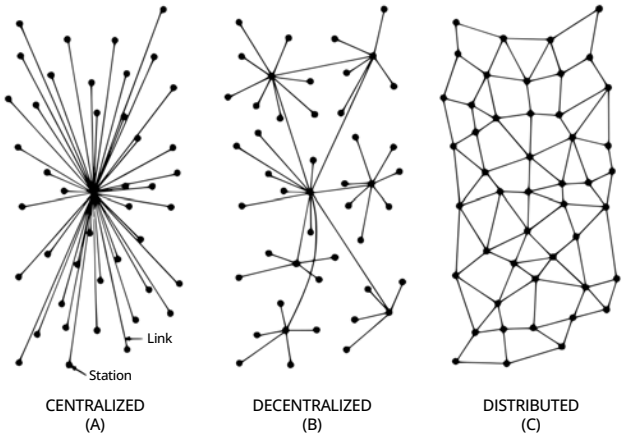
Bitcoin's decentralization can be thought of as a synergetic musical orchestra, a balancing act where all the different musicians make the most beautiful music together. There is no boss in the Bitcoin network; instead, miners, nodes, users, developers, and projects perform their roles with autonomy and collaboration.

The decentralized ledger, maintained by nodes, guarantees transparency, while the proof-of-work mechanism provides security and deters centralization in mining. Users experience financial sovereignty and empowerment free from the control of the fiat system. Developers, guided by consensus, ensure the protocol adapts to meet the evolving needs of humanity. Bitcoin projects, in their own unique ways, contribute to the broader mission of collective freedom.

An Introduction to Bitcoin

As you can see, every participant plays a vital role in shaping Bitcoin's adoption and empowering humanity. Each participant in this decentralized orchestra contributes to the resilience and longevity of Bitcoin, creating a trust-free, borderless, and empowering ecosystem.

In summary, the symphony of decentralization in Bitcoin resonates as a testament to Satoshi Nakamoto's vision and the immense passion of a global community seeking freedom and empowerment.



Class Exercise — Consensus Building in a Peer-to-Peer Network

Objective

To understand how consensus is achieved in a group and learn about cryptography and the consensus layer of Bitcoin.

Materials

Message with encrypted and unencrypted instructions for actions ("attack" or "do not attack").

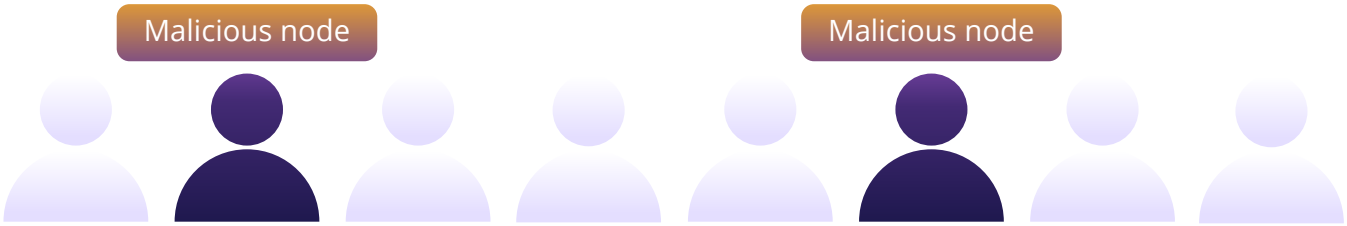
Activity Preparation

The teacher will select a group of three or four students before class to be malicious nodes in the following activity. The teacher will assign these malicious nodes a cryptographic puzzle as homework in the previous class.

Exercise Steps:

1. The teacher will select one student in the group as an “originator” who will receive a message on a piece of paper that says "ATTACK" and a series of numbers that says, "4-16-14-21-1-21-21-1-3-11-”.

2. The students will form a circle in the designated space, ensuring the selected students who will be malicious nodes are separated to improve the effectiveness of the lesson.



3. Once the group has formed a circle, the originator will pass the note to the individual to the right side of the circle.

4. After everyone has read the message, the originator will give the signal to the group by saying “now,” and the group will react to the message simultaneously. If the message reads “ATTACK,” then all participants will take a step forward.

5. After the initial reaction, some students (those who received the encrypted message and interpreted it correctly) will remain still, while the rest will follow the original instruction, revealing a lack of consensus.

Conclusion:

Discuss why consensus was not achieved, introducing the concept of the Byzantine Generals' Problem, how it relates to the need for a common goal, and later discussing how Bitcoin provides a solution to this problem.

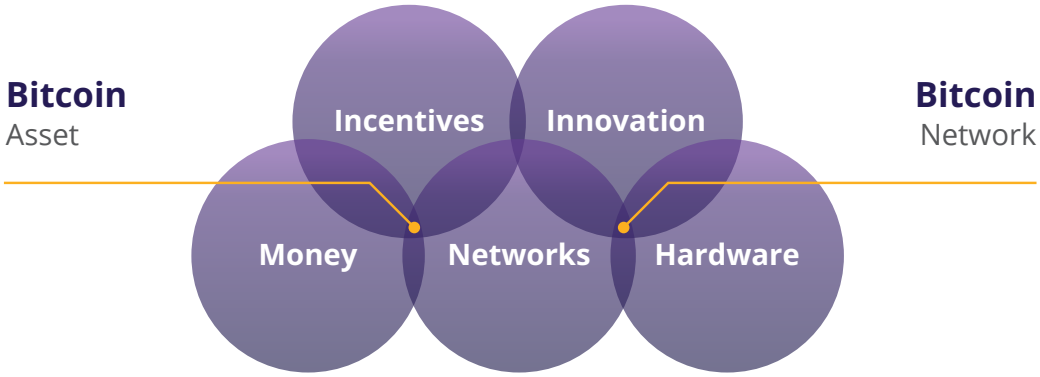
6.2 Bitcoin as Sound Digital Money

6.2.1 Introduction

Activity:
Watch 1.5 min video, "What Is Bitcoin?

In simple terms, Bitcoin is money. Bitcoin is not an investment but rather a safe, empowering way of saving your hard-earned money.

Having bitcoins won't make you rich because it won't give you a return of more bitcoins. Its value, measured against a fiat currency, does go up, but this is only because of its growing adoption and the devaluation of fiat currencies.



Bitcoin is a new form of money; it is, "The Internet of Money," which means that it is open for anyone to join and start exchanging value with other users. Even the most isolated and poor communities in the world finally have access to a monetary system. Just like everyone who has a phone and an internet connection can use a search engine, Bitcoin makes it possible for everyone with a phone and internet connection to access a new, global monetary system.

Faster, Cheaper Payments

Send money across the globe in minutes, with extremely low fees.

Financial Inclusion

2.5 billion unbanked people can access money via a phone or computer.

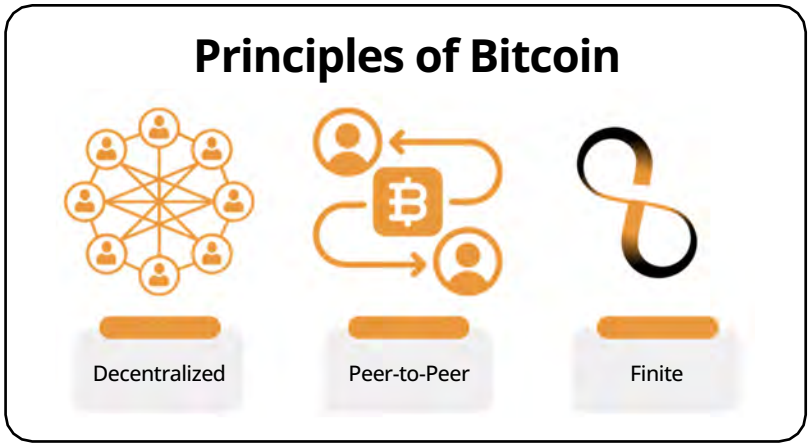
Increased Privacy

Bitcoin transactions are public but your identity is not.

Bitcoin is completely digital and borderless. It doesn't matter where you are located because it lives on computers and smartphones from all over the world. Lots of users worldwide run the Bitcoin software and a copy of its ledger.

This software and record of all transactions has a very low chance of disappearing as there are countless copies of it. To shut it down, you would need to shut down the entire internet, forever, which is extremely unlikely to happen.

Finally, Bitcoin is scarce, which means that the number of bitcoin tokens that can exist is absolutely limited. No one can counterfeit Bitcoin — not even the most powerful governments and financial institutions.



6.2.2 Bitcoin's Features

The Evolution of Sound Money

As you learned in Chapter 2, the lifecycle of sound money progresses through three stages to receive general acceptance from society: from being a store of value to becoming a medium of exchange and, finally, a unit of account.

The first stage of money, a store of value, is when a currency starts gaining trust as a stable (or appreciating) asset over time. People who recognize this early seek to protect their wealth by storing it in this form of money, especially during a time of geopolitical and macroeconomic uncertainties.

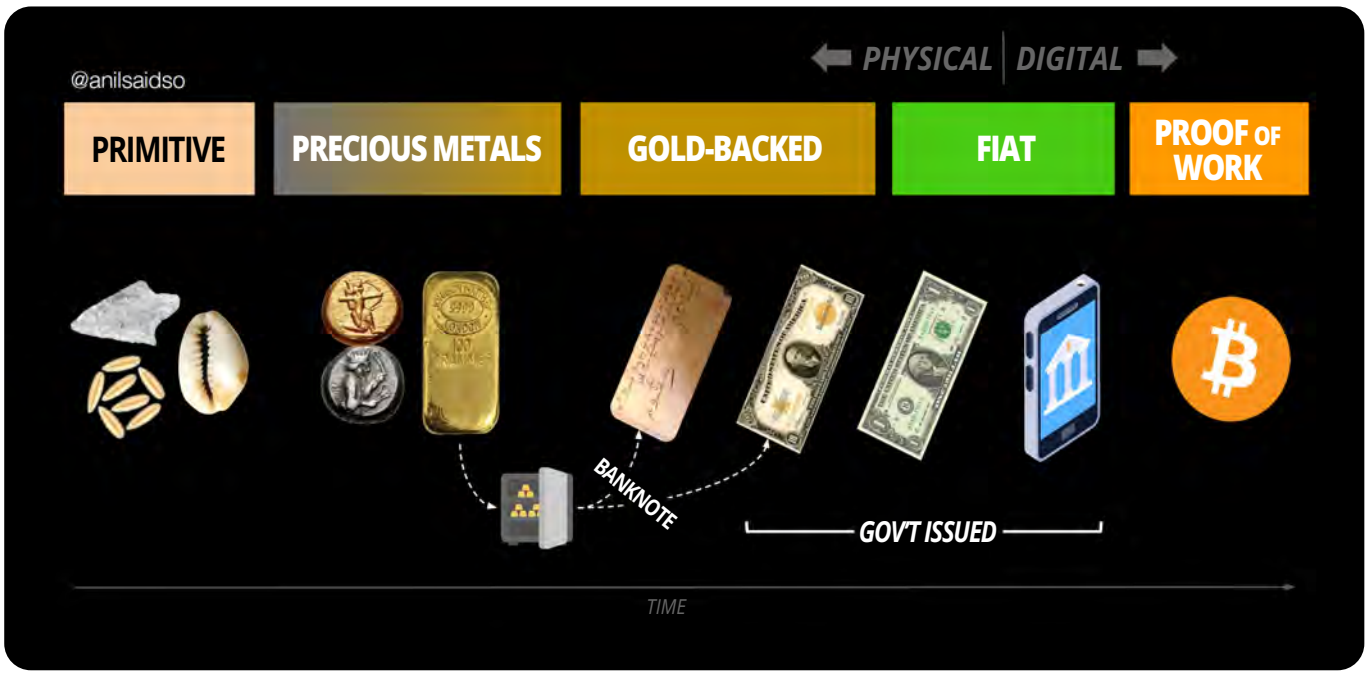
Some groups, like media outlets, call Bitcoin a form of "digital gold." This is because Bitcoin firmly established itself as a store of value during the past decade. Every day, more and more people start to view Bitcoin as a hedge against inflation, like gold was historically.

The next stage is when confidence in a currency's stability solidifies. This is when the currency transitions into a medium of exchange, facilitating transactions in people's daily lives. During this stage, the currency starts to become widely accepted for the exchange of goods and services.

Bitcoin is progressively moving toward becoming a medium of exchange. With growing merchant acceptance and the development of the protocol, Bitcoin transactions are becoming more efficient and commonplace in daily commerce. One example of this is El Salvador, where Bitcoin is officially recognized as legal tender. Each day, more and more ordinary citizens and businesses are using Bitcoin as a medium of exchange.

In the final stage, a currency achieves the status of a unit of account, serving as a common measure for pricing goods and services. This is the stage in which it becomes the standard metric against which all other values are measured.

The journey toward becoming a unit of account is a more extended (long-term) process. The world currently measures goods and services only in fiat currencies, therefore, Bitcoin needs broader adoption and integration into various financial systems. However, the foundation is already laid as businesses and individuals begin to consider and denominate values in Bitcoin.



As you can see, Bitcoin is well on its way in this evolutionary cycle of sound money. When Bitcoin becomes fully integrated into the global financial system, it could become a standard unit of account, reshaping the entire global monetary system.

Properties of Money

As you learned in Chapter 2, over time, humanity has figured out that real sound money must possess certain properties to be effective. These properties are durability, divisibility, portability, acceptability, scarcity, and fungibility.

Let's see if Bitcoin passes the test.

Durability: Bitcoin is purely digital and thus completely durable.

Divisibility: For comparison, the fiat currency USD can be divided to the cent (.01). Bitcoin can be divided into what is known as a satoshi or sat (.00000001). And because of Bitcoin's digital character, it can be divided even more in the future if humanity needs it. Bitcoin is currently the most divisible monetary asset in the world.

Portability: In April 2020, $1.1 billion was transferred in just a few minutes, and it only cost 68 cents. No other way of paying can move that much money at such a low cost so quickly, and all on its own. This is what makes Bitcoin the most easily movable form of money in the world.

Acceptability: Bitcoin is still in its early stages of becoming a medium of exchange, and compared to fiat currencies, acceptability is currently low.

Scarcity: There will only ever be 21 million bitcoins in existence. By code, it is impossible for this amount to ever increase, which means that Bitcoin is not only scarce but the scarcest monetary asset in the world.

Fungibility: Each unit of bitcoin is the same as any other unit and can be interchanged and transacted over the Bitcoin protocol on a like-kind basis, which makes it a fungible currency.

An Introduction to Bitcoin

Bitcoin vs. Gold vs. US Dollar

Properties of Money	Gold	Fiat	Bitcoin
Durability	High	Moderate	High
Portability	Moderate	High	High
Divisibility	Moderate	Moderate	High
Fungibility	High	High	High
Scarcity	Moderate	Low	High
Verifiable	Moderate	Moderate	High
Established History	High	Moderate	Low
Censorship Resistant	Moderate	Moderate	High
Smart/Programmable	Low	Moderate	High

"Bitcoin vs Gold vs US Dollar" Bitcoin Magazine, https://bitcoinmagazine.com

Bitcoin is a type of smart money that's programmable, can't be taken away, and has all the qualities that make it great for saving and easy for merchants who want fast transactions.

Since it's a transparent digital ledger, Bitcoin can be super efficient in catching fraud and figuring out risks in its services. It has the good aspects of gold, such as there only being a limited amount of it, but it also has the benefits of fiat currencies because you can divide it and carry it around easily. Plus, it brings in new features that work well in our digital world.

What do you think? Bitcoin is not yet widely recognized and adopted, but is it sound money?

Activity: Class discussion - Is Bitcoin Sound Money?

Now that we have discussed Bitcoin in greater detail, let's look at our money comparison table from Chapter 2 again and see how Bitcoin compares with other forms of money:

Characteristic of Good Money	Cows	Cigarettes	Diamonds	Euros	Bitcoin
Durable					
Portable					
Uniform					
Acceptable					
Scarce					
Divisible					
Total					

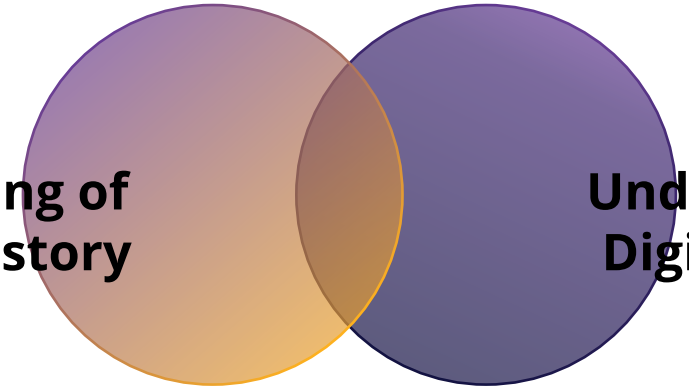
6.2.3 Embracing Personal Responsibility

> The result is a distributed system with no single point of failure. Users hold the crypto keys to their own money and transact directly with each other, with the help of the P2P network to check for double-spending.
>
> **Satoshi Nakamoto**

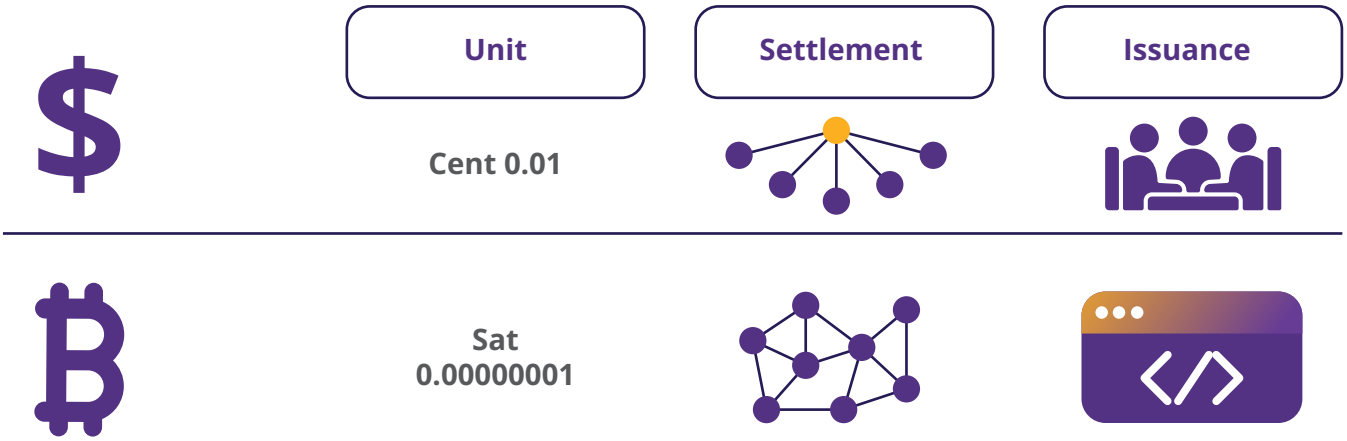
An Introduction to Bitcoin

In the fiat world, people rely on governments, banks, and established payment providers. The heads of these (financial) institutions set the rules of the network, and the participants, mostly ordinary citizens, must comply with these rules. It doesn't matter where you live - there are always a set of standard procedures that instruct you on what to do and how to do it. Over time, this led to a cycle of hardship, particularly for families that struggle with the increasing challenges of daily life.

Because of this system, people are accustomed to putting the responsibility for their finances in the hands of others. For example, most people rely on someone else to help them, especially when something goes wrong (like losing access to your bank account).



As you know, the monetary system of Bitcoin is very different. Bitcoin operates in a specific way, and rulers have been replaced by an autonomous system of rules. There is no dictator or leader, which also means that no one will dictate to you what you need to do. If you want the newfound freedom and empowerment of Bitcoin, you will need to learn how it works and integrate the technology in a way that works for you personally.



With Bitcoin, you are fully in control of your funds, but with this additional control comes increased responsibility. For example, losing access to your bitcoins by losing your keys to your digital wallet means you have lost your savings — permanently. There's no customer service hotline to call or someone else to turn to - when there is a problem, you need to take care of it yourself.

Fortunately, this will not happen to those who decide to take full responsibility over their own lives. Using Bitcoin is not inherently complicated; it’s just a new concept. Any discomfort arises because it's unfamiliar, but if you are willing to learn how to use Bitcoin and fully embrace the responsibility of safeguarding your wealth, Bitcoin becomes an empowering tool — you are in control, and no one can seize your wealth.

In summary, the key lies in action, understanding Bitcoin's workings, and implementing it according to your unique needs and life philosophy. Next, we’ll begin to use bitcoins by setting up a Bitcoin wallet, sending and receiving our first transactions, and reviewing security best practices.

Chapter #7

How to Use Bitcoin

7.0 Introduction

7.1 Acquiring and Exchanging Bitcoin

- **7.1.1** P2P: Physical
- **7.1.2** P2P: Online
- **7.1.3** Centralized Exchanges

7.2 An Introduction to Bitcoin Wallets

- **7.2.1** Self-Custodial vs. Custodial Wallets
- **7.2.2** Different Types of Bitcoin Wallets
- **7.3.3** Open Source vs. Closed Source
- **Activity:** Class Evaluation of Bitcoin Wallets

7.3 Setting Up a Mobile Bitcoin Wallet

- **Activity:** Setting Up/Recovering a Bitcoin Wallet

7.4 Receiving and Sending Transactions

- **Activity:** Bitcoin Transactions in Action

7.5 Saving in Bitcoin

7.6 Don't Trust, Verify

Student Workbook

English Version | 2025

How to Use Bitcoin

7.0 Introduction

> Why would anyone trust nerd money vs. central bank money? Nerds brought you the internet. Banks brought you the Great Depression.
>
> **Andreas M. Antonopoulos**

Now that we have a better understanding of what Bitcoin is and its purpose, it's time to learn how to use it practically. In this chapter, we'll guide you through the process of acquiring bitcoins step-by-step, explore the various types of wallets available, help you set up your own Bitcoin wallet, and even practice sending and tracking a bitcoin transaction on the network. It's time to turn your understanding into action!

7.1 Acquiring and Exchanging Bitcoin

There are many ways to acquire bitcoin. For example, you can:

- Get paid in bitcoins in exchange for your work and pay for other people's products and services with bitcoins (more on that in Chapter 8)
- Mine bitcoins (more on that in Chapter 9)
- Exchange your fiat currency for bitcoins or exchange your bitcoins for fiat currency in person.
- Exchange your fiat currency for bitcoins or exchange your bitcoins for fiat currency online.

Below, we'll explore exchanging fiat currency for bitcoins and vice versa, both through in-person transactions and online methods, as they are the most common options.

7.1.1 Peer-to-Peer: In Person

Engaging in peer-to-peer (P2P) transactions to acquire and sell bitcoin involves directly exchanging your fiat currency (or any other goods or services) for bitcoins with another individual, eliminating the need for a bank or other party to be involved in the transaction.

Both parties mutually determine the exchange amount and rate. The buyer provides the cash, the seller transfers the bitcoins, and the transaction concludes. While it's easier to do P2P exchanges physically by meeting with the other individual directly in the real world, you can also do so from virtually anywhere thanks to the internet. Additionally, exchanging bitcoins for fiat currency follows a similar process in reverse.

7.1.2 Peer-to-Peer: Online

Enter P2P platforms, where Bitcoin buyers and sellers meet in cyber space to conduct transactions without any intermediaries, directly on the internet.

With such platforms, you don't have to trust anyone with your information or money; you can meet other peers and trade with them directly.

On most P2P platforms, peers have to escrow some of the funds to ensure they will comply with their part of the deal. Escrow means putting the money in a safe place that the platform controls until both parties do what they promised. It's like a trusted friend holding onto your stuff until everyone keeps their word.

7.1.3 Centralized Exchanges

Using centralized exchanges may be the easiest way to acquire and sell bitcoins but it also involves significant trade-offs. Centralized exchanges are companies that allow clients to buy and sell bitcoins directly through them. However, this convenience comes at a cost.

CENTRALIZED

Centralized Exchanges and Their Trade-Offs

It's important to note that when buying bitcoins through a centralized exchange, you are often required to provide personal information and verify your identity. This creates a risk of identity theft and exposes your personal information to potential threats. Additionally, centralized exchanges hold your bitcoins for you, which means you are not in control of your money until you withdraw it from them.

To add to these concerns, centralized exchanges can misappropriate users' funds or lend more bitcoins than they have in reserves until they collapse. Yes, just like banks! However, in the Bitcoin world, there is no central bank to bail out fraudulent banks by printing more currency because you can't print more bitcoins!

7.2 An Introduction to Bitcoin Wallets

Unlike physical money, bitcoins are not actually present in a Bitcoin wallet. Instead, they live on the distributed ledger that the Bitcoin network constantly verifies and secures. So, how can you own bitcoins?

You have ownership of your bitcoins only when you own the private keys allowing you to sign transactions and transfer ownership of your bitcoins to someone else. This is the act of sending bitcoins.

With that in mind, let's take a look at two concepts we describe when using the term **"wallet":**

- A master private key (like a password) from which you can generate public keys that you can share with others to receive and send bitcoins.
- The mobile or desktop interface from which you can interact with the Bitcoin network to retrieve your bitcoin balance, send and receive transactions, and broadcast them to the network. Different types of wallets, along with their benefits and tradeoffs, will be described in the next section.

7.2.1 Self-Custodial vs. Custodial Wallets

Before detailing the different types of Bitcoin wallets and their characteristics, let's make an important distinction between self-custodial and custodial wallets, as shown in the table below. You can see the benefits and risks of using each wallet type and who controls the bitcoins in each case. Self-custodial means the user holds the private keys, which means they are in true possession of their bitcoins, while in the second type, a third party, holds their bitcoins.

Wallet Type	Who controls my bitcoin?	Benefits	Risks
Self Custodial Wallets	**The user**	Complete control over funds and transactions, no approval process or account freeze, no corporate or government control, protected against arbitrary confiscation, like keeping money at home.	No recovery if recovery phrase is lost, less customer support, full responsibility falls on the user.
Custodial Wallets	**The third-party provider**	Easy recovery if access is lost, easier customer support	Funds are always connected to the internet, so more vulnerable to hacking and breaches. Custodians control and can freeze accounts.

In a self-custodial wallet (also called non-custodial wallet), you are the only one with the keys to the wallet and you have full control over what goes in and out. On the other hand, in a custodial wallet someone else holds the private key, giving them full access to move any bitcoin that wallet controls on your behalf.

- Self-custody is like being your own bank. Transactions are not subject to control or authority by any government or company, but it also means you bear full responsibility for keeping your bitcoins secure.
- Self-custody ensures that third parties cannot confiscate your bitcoins without your consent.
- Self-custody gives peace of mind in times of uncertainty, knowing your bitcoins are secure.

It's important to choose the right type of wallet for each individual's needs. Sometimes, people find it hard to distinguish whether they are installing a self-custodial or a custodial wallet. This table shows the differences with the installation process.

Wallet Type	Step 1: Choose a Wallet	Step 2: Install the Wallet	Step 3: Create a New Wallet	Step 4: Secure Your Seed Phrase	Step 5: Start Using Your Wallet
Self Custodial Wallets	Choose a self-custodial wallet provider	Follow the wallet provider's instructions	Generate a **recovery phrase** and at least one **private key**	Store the **recovery phrase** in a secure location	Start using the wallet to receive and send **bitcoins**
Custodial Wallets	Choose a custodial wallet provider	Follow the wallet provider's instructions	Create an account with the wallet provider	N/A (wallet provider holds the **private keys**)	Start using the wallet to receive and send **bitcoins**

"Not your keys, not your coins" is a popular saying among bitcoin holders. It refers to the idea that if you don't have direct control over the private keys associated with your Bitcoin wallet, you don't have true ownership of the coins.

Whoever accesses your private keys will gain ownership of your bitcoins. This is why it is of the utmost importance to protect them by keeping them away from prying eyes! We'll see a few ways you can do that later in the book.

For what follows, we'll be talking about self-custodial wallets only, where the user owns their keys and has complete control over their bitcoins.

Don't worry if it seems complicated or you don't understand everything - this is a journey, and you will understand more as you start using Bitcoin more!

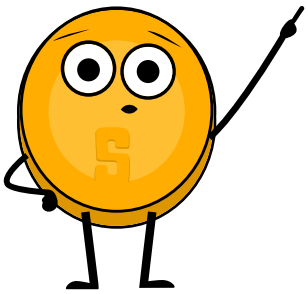
7.2.2 Different Types of Bitcoin Wallets

Depending on where your private key is created and stored, we commonly use different names to describe Bitcoin wallets. If the keys are stored on your smartphone, we call it a "mobile wallet." If they're stored securely on a dedicated device, we call it a "hardware wallet." If the key is only stored on paper, then it is called a "paper wallet."

The different names we give to Bitcoin wallets depending on their structure:

Wallet Type	Description	Advantages	Disadvantages	Example User
Online Wallet	A wallet accessed through a web browser.	Accessible from any device with an internet connection. Easy to use.	Less secure. Can be hacked or compromised.	Someone who needs to access their wallet frequently and doesn't have a lot of funds to store.
Mobile Wallet	A wallet installed on a mobile device.	Convenient. Can be accessed from anywhere.	Can be lost if the device is misplaced, stolen, or hacked.	Someone who needs to make transactions on the go and doesn't have a lot of funds to store.
Desktop Wallet	A wallet installed on a desktop computer.	More secure than online wallets. Can be used offline.	Can be hacked if the computer is infected with malware.	Someone who wants to store a large amount of **bitcoins** and is comfortable with using a desktop computer.
Hardware Wallet	A physical device that stores **bitcoins** offline.	Very secure. Can be used offline.	Funds could be unrecoverable if the device is lost or stolen.	Someone who wants to store a large amount of **bitcoins** and is willing to pay for the added security of a hardware wallet.
Paper Wallet	A physical record of a Bitcoin wallet's private and public keys.	Very secure. Can be used offline.	Can be lost or stolen if the physical record is lost or stolen.	Someone who wants to store a large amount of **bitcoins** and is willing to take added precautions to ensure its security.

Because the keys can be moved from one device to another, the “status” of your Bitcoin wallet is not definitive. For example, if I generate the keys of my Bitcoin wallet on a computer and later upload them to my phone, the “desktop wallet” then becomes a “mobile wallet.”



When it comes to storing your bitcoins, it’s not just about who has control over them — there are many other risks to consider. That’s why it’s important to find a storage solution that is both secure and convenient.

When you analyze the trade-offs of the various types of wallets, you will learn that there is no ideal wallet to satisfy all needs.

When choosing a Bitcoin wallet, there are several things you should consider:

- **Security:** Make sure the wallet has strong security measures in place such as two-factor authentication and secure password policies.
- **Privacy:** Consider whether the wallet allows you to remain anonymous or if it requires personal information to set up an account.
- **Ease of use:** Choose a wallet that is easy to use and navigate, especially if you are new to Bitcoin.
- **Compatibility:** Make sure the wallet is compatible with your device and operating system.
- **Fees:** Compare the fees charged by different wallets to make sure you are getting the best deal.
- **Reputation:** Research the reputation of the wallet and its team to make sure it is trustworthy.
- **Control:** Some wallets give you more control over your private keys, which can be a security advantage.

Consider whether you want a wallet that gives you full control or one that is more user friendly but may have less control.

7.2.3 Open Source vs. Closed Source

Another important factor to keep in mind when choosing a Bitcoin wallet is knowing if the application or software is open-source.

Open-source code is very important because it allows the community to review the code and continue developing the project if the team were to stop working on it.

Just as Bitcoin's code is completely open for everyone to review, use, and modify, so should be the code of the wallet you use to store your bitcoins.

Activity: Class Discussion and Evaluation of Bitcoin Wallets on bitcoin.org

Go to the following website:

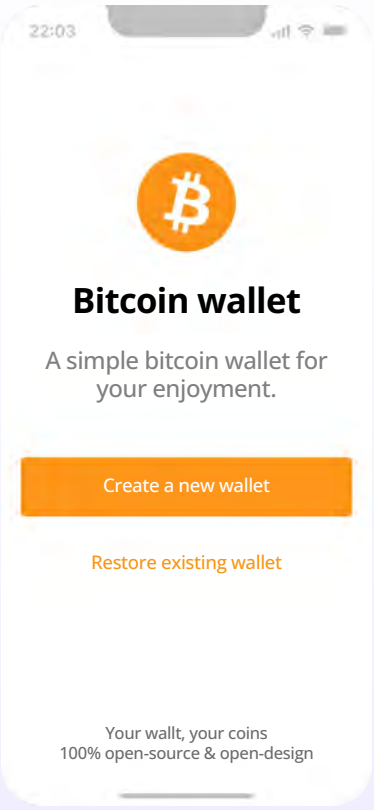
https://bitcoin.org/en/choose-your-wallet and use your new knowledge of Bitcoin wallets to select the best one based on the criteria we discussed today.

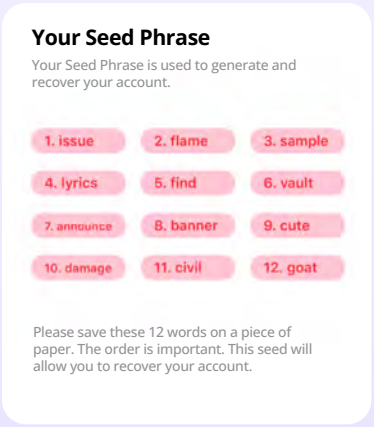
7.3 Setting up a Mobile Bitcoin Wallet

Now that we have a better understanding of Bitcoin wallets and the differences between them, we'll see how to use one in practice. For this example, we'll create a mobile wallet directly on our smartphone.

Activity: Setting Up/Recovering a Bitcoin Wallet

If students do not have cell phones, the teacher will provide one for student to borrow. There are two options for this activity.





Class Exercise: Option 1 — Download a new wallet.

How to create and use a Bitcoin wallet:

1. Search for the app in the App Store (iOS) or Google Play Store (Android).
2. Open the app and type in your 12- or 24-word recovery phrase (sometimes called a seed phrase). **Be sure to write it down and keep this in a safe place!** This recovery phrase allows you to recover full access to your funds if needed.

Remember that if you lose or forget this sequence of words, you will not be able to access your bitcoins if you lose access to your wallet.

3. You must then confirm that you have actually saved your recovery or seed phrase. To do this, you must enter, in the same order, the words of your seed phrase.
4. As an additional measure of security, some wallets allow you to choose a secure password. Your private key and first Bitcoin address are automatically created for you by your wallet.

Think of your public key as your email address — you want to share this with others so that they can send you bitcoins — or, in the case of an email address, an email.

Think of your private key as the password to your email – you wouldn't want to share this with anyone, as it would give them access to your email.

5. Use your "receive" address to receive bitcoins. Transfer bitcoins to your wallet. With a self-custodial wallet, you cannot always buy bitcoins directly with fiat, so you might need to purchase and transfer them from an exchange first.

Class Exercise: Option 2 - Restore a wallet (Time-Limited).

Download a Bitcoin wallet and add some satoshis for each student.

Give each student a sheet with a seed phrase to retrieve a wallet.

Guide students step-by-step:

1. When you first start your wallet, you will see three methods of wallet creation, tap **[Import an existing wallet].** You will see an introduction screen, tap **[Restore with recovery phrase].**
2. Enter your 12/18/24-word recovery phrase one by one, in the correct order.
3. Touch **[Restore]** when finished.
4. You will see an "Import Successful" message when your wallet has been successfully imported.

7.4 Receiving and Sending Transactions

A bitcoin transaction is a transfer of ownership of existing bitcoins to a new owner. However, instead of transferring actual coins, all the nodes in the network update their local copy of the public ledger to reflect the change in ownership.

When sending a bitcoin transaction, the sender signs a message that only they can sign with their private key, signaling to the network that the ownership of the bitcoins has changed to the recipient's address.

The bitcoins will now be tied to an address that only the new owner can send from, giving them ownership of the bitcoins.

LEDGER

Account Owner	Value
Sam	2.50
Adam	3.00
Michael	6.00
Jim	1.50
Robert	2.00
Eliana	1.75
Daniel	5.25

Bitcoin Transaction Request Message
Jim sends
0.50 BTC to Eliana

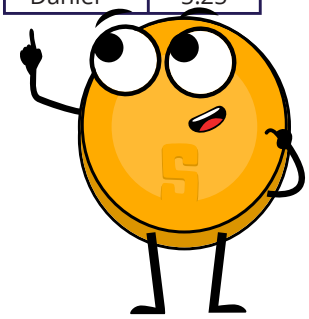
Jim ▸ Eliana
0.50 BTC

LEDGER

Account Owner	Value
Sam	2.50
Adam	3.00
Michael	6.00
Jim	1.00
Robert	2.00
Eliana	2.25
Daniel	5.25

New bitcoin transactions are initiated from wallets around the world, but there is no central payment processor. Instead, miners around the world compete to record transactions in the ledger.

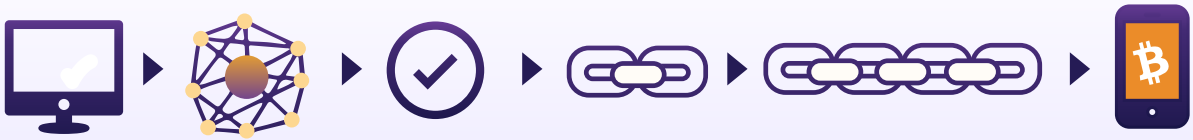
Let's say Jim owes Eliana 0.5 BTC and is ready to pay her back. Both have digital wallets.



1. Eliana shares her address with Jim.
2. Jim uses his wallet software to create the transaction, which includes Eliana's address, the amount to be transferred (0.5 BTC), and a fee for the miner.
3. After signing the transaction, it is broadcast to the network, where it is verified by nodes. Nodes check the transaction for validity and ensure that Jim has enough funds. If he does not, they reject the transaction immediately.
4. Once the transaction is verified, miners add it to the blockchain and the funds are transferred to Eliana's address.
5. Eliana can then use her private key to access the transferred funds in her wallet.

It's important to note that once the transaction is complete, it cannot be reversed.

How a Bitcoin Transaction Works



Someone requests a transaction | Transaction broadcasted to P2P computers (nodes) | Miners verify the transaction | Transactions combined to form a data block | New block added to the existing blockchain | The transaction is complete

Receiving Bitcoin Transactions:

To receive bitcoins, you will need to provide the sender with your Bitcoin wallet address. This is a unique string of letters and numbers that represents your wallet and is used to identify it on the Bitcoin network. You can find your wallet address by logging into your Bitcoin wallet and looking for an option to "Receive" or "Deposit" bitcoins.

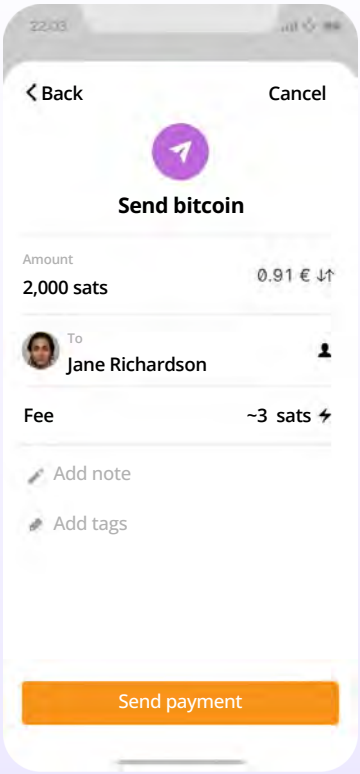
You can then share your Bitcoin address with the sender in one of several ways:

1. Copy and paste the address: You can copy the address by highlighting it and pressing "Copy" on your keyboard, then paste it into an email or message to the sender.
2. Share a link to your Bitcoin wallet: Some Bitcoin wallets allow you to create a link to your wallet that you can share with the sender. They can then click on the link to access your wallet and send the bitcoins.
3. Share a QR code: If the sender has a smartphone with a Bitcoin wallet app, they can scan the QR code to get your Bitcoin address.

How to Use Bitcoin

Once the sender has your Bitcoin address, they can send you bitcoins by entering your address and the amount they want to send you and initiate the transaction. The bitcoins will then be sent to your wallet and will be visible once the transaction is confirmed on the Bitcoin Network. This usually takes a few minutes.

Next, we will take a look at sending bitcoin transactions.



Sending Bitcoin Transactions:

To send bitcoins, you will need a few things: a Bitcoin wallet, the recipient's Bitcoin address, and the amount of bitcoins you want to send.

1. Open your Bitcoin wallet. An SMS code will be sent to your phone number, and you will need to enter it in the dialog box. Alternatively, if you have enabled Google 2FA, you will need to enter the six-digit code from the Google Authenticator app.
2. Navigate to the "Send" or "Withdraw" feature and copy the recipient's address.
3. Enter the recipient's Bitcoin address by pasting it in the "To" field.
4. Enter the number of bitcoins you want to send in the "Amount" field.
5. Double-check the recipient's address and the amount to be sent.
6. Before clicking "Confirm and Send," we recommend you double-check the transaction details one more time to ensure that you are sending the correct amount of bitcoins to the correct wallet address.
7. Confirm the transaction and wait for the network to confirm the transaction

Now you know how to evaluate, select, and set up a self-custodial Bitcoin wallet. Sending bitcoins from one wallet to another on the Bitcoin network is called sending an "on-chain" transaction. This is because the transaction occurs on the main Bitcoin network blockchain. On-chain transactions are the safest way to transact with bitcoins. However, on-chain transactions are slower and can be significantly more expensive than other options, such as the Lightning transactions we will discuss in Chapter 8.

Activity: Bitcoin Transactions in Action

Objective: To understand the underlying concepts and mechanics of a peer-to-peer bitcoin transaction.

Before we get started, here's a quick reminder on the key players in a bitcoin transaction:

- Senders and receivers are the parties who wish to transact with each other.
- Nodes validate transactions and store a complete copy of the blockchain. *Light nodes let people validate transactions while using less storage and fewer computational resources.
- Miners are responsible for adding new transactions to the blockchain.

Understand your role. You have been assigned one of the following: sender, receiver, node, or miner.

- Senders will be responsible for creating and broadcasting transactions.
- Receivers will be responsible for receiving and verifying transactions.
- Nodes will be responsible for validating the transactions.
- Miners will be responsible for adding the transactions to the blockchain.

Both nodes and receivers have to verify transactions

1. **As a sender:** Create a transaction.

To create a transaction, follow these steps: Take a transaction note and write the number of coins you want to send and the name or initials of the receiver. Sign the note with your name or initials, simulating a private key. Pass the transaction note and the corresponding number of coins to the receiver.

2. **As a receiver:** You are responsible for verifying the transactions. Follow these steps:
   - Check the transaction note to ensure that the correct number of coins and the receiver's name or initials are written.
   - Count the coins received and compare them to the number of coins written on the note.
   - If the coins match, check the approval box. If the coins do not match or you have doubts, reject the transaction.

Coin Sent	Sender	Sender Signature	Receiver	Date & Time	Recipient Approval

3. **As a node:** Verify and validate transactions. You are responsible for checking that the transaction is valid.
   - Verify that the sender's address and the receiver's address are valid.
   - Check that the sender has enough funds to complete the transaction and that the transaction does not double-spend any coins.

Coin Sent	Sender	Sender Signature	Receiver	Date & Time	Node Approval

How to Use Bitcoin

4 **As a miner:** You are responsible for adding the transactions to the blockchain. Follow these steps:

- Check the transactions that have been approved by the receivers and validated by the nodes.
- Roll the dice and compare the numbers with the other miner. The miner with the smaller number will add the transaction to the blockchain.
- For your time, energy, and effort, you will earn a point. At the end of the activity, the miner with the most points wins.

**Once a transaction is added to the blockchain, it cannot be changed or reversed.

5 **Keep track of your coin balance:** Throughout the activity, keep track of your coin balance by counting the coins in your digital wallet.

Coins Sent	Sender	Sender Signature	Reciver	Date & Time	Approval

6 **Discuss the concepts learned with your class.**

7.5 Saving in Bitcoin

Bitcoin is a way to safeguard your money against inflation and protect it from being controlled by anyone else, if you do it correctly. Saving in bitcoins provides a vehicle to store, accumulate, and build wealth over time. As you understand by now, the type of money you choose to save is one of the most important decisions you can make. Choosing wisely allows you to build a better future for yourself and your family.

Peace of Mind: When stored properly, Bitcoin is the only form of property no one can take away from you.

7.6 Don’t Trust, Verify

Whatever you do in Bitcoin, remember this: “Don’t Trust, Verify.” There are no leaders in Bitcoin. You should never blindly follow someone’s claims. Rather, you should always question what you’re being told and verify it for yourself. By following this mantra, you’ll protect yourself from losing your bitcoins. This goes for claims such as “the next Bitcoin” just as it does for “investment opportunities” or promises of “quick and easy profits.”

In summary, Chapter 7 has given you the important skills to use Bitcoin in your everyday life. You have learned how to get and exchange bitcoin in different ways and how to keep it safe using various wallets.

By setting up your mobile Bitcoin wallet and making transactions with others, you now have the hands-on experience to confidently use Bitcoin day-to-day. By understanding Bitcoin as a way to save money and following the idea of “Don’t Trust, Verify," you're now in control of your money.

In the upcoming chapter, we will explore the Lightning Network. We will look at how this innovative technology is changing the way people worldwide access and use money. From everyday transactions to more advanced applications, you will learn how the Lightning Network empowers individuals, communities, and businesses by providing them access to financial services.

Chapter #8

Lightning Network: Using Bitcoin in Your Daily Life

8.0 Introduction

Activity: Watch “Bitcoin Lightning Network Explained: How It Actually Works”

8.1 The Lightning Network

8.2 Different Types of Lightning Wallets

8.2.1 Self-Custodial vs. Custodial Wallets

8.2.2 Open Source vs. Closed Source

8.3 Setting Up a Bitcoin Lightning Wallet

8.4 Sending and Receiving Lightning Transactions

Activity: Lightning Wallet Relay Race

8.5 Buying Coffee and Groceries with Bitcoin

8.5.1 Online: Payment Plugins — Ecommerce

8.5.2 In Person: Find a Merchant in Your Area

8.5.3 Transitional Tools: Gift Cards and Payment Cards

8.5.4 Circular Economies and Bitcoin as a Medium of Exchange

Student Workbook

English Version | 2025

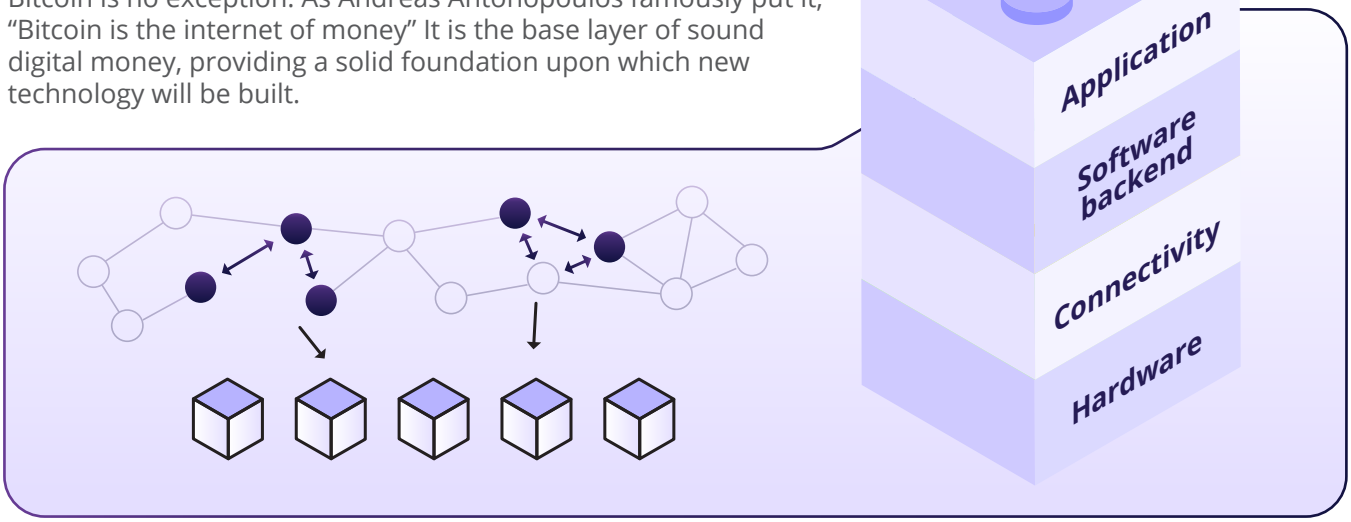
Lightning Network: Using Bitcoin in Your Daily Life

8.0 Introduction

> We're building the Visa network for bitcoin. But what I think is powerful, is unlike Visa, anybody can build on top of it.
>
> **Elizabeth Stark**

Technologies typically grow and expand in layers, like a stack. Think of your favorite website, email, or social media: they were built on top of the internet protocol, which was built on top of computers, which were built on top of electricity, and so on. These technologies started out with a very simple design and continued to improve over time.

Bitcoin is no exception. As Andreas Antonopoulos famously put it, "Bitcoin is the internet of money" It is the base layer of sound digital money, providing a solid foundation upon which new technology will be built.

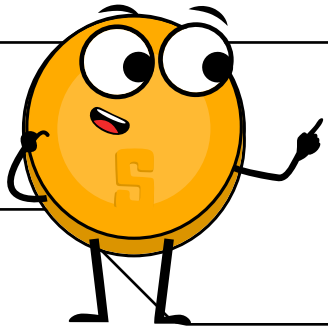


One of these layers is called the Lightning Network. This is like a super-fast highway for Bitcoin, helping people send and receive bitcoins quickly and with very low fees. It allows users to make instant, small transactions on top of the regular Bitcoin network. This makes buying a coffee or paying a friend simple and fast!

Remember: A satoshi is like the smallest coin of bitcoin. Just like a dollar can be broken into cents, one bitcoin can be split into smaller units called satoshis. One bitcoin equals 100 million satoshis, making satoshis the tiniest bits of value in the Bitcoin system. In this chapter, when we talk about sending bitcoins through the Lightning Network, we'll call it "sending sats," which are just smaller parts of a bitcoin.

Sats	Bitcoin
1	0.00000001
10	0.00000010
100	0.00000100
1,000	0.00001000
10,000	0.00010000
100,000	0.00100000
1,000,000	0.01000000
10,000,000	0.10000000
100,000,000	1.00000000

Activity: Watch this video on the Lightning Network



8.1 The Lightning Network

As we've just seen, the Lightning Network serves as a payment system, facilitating quick and cost-effective transactions with bitcoins. It operates by establishing a shared wallet where both parties hold some bitcoins. They can conduct numerous transactions with each other without the need to record each one on the main ledger. The final balance is then recorded on the ledger once the transactions are complete.

The Lightning Network is a payment system that allows users to send and receive payments quickly and inexpensively using bitcoin. It works by setting up a shared wallet where both people store their bitcoins and then making unlimited transactions with each other without touching the main blockchain. When they're done, the final balance is recorded on the main blockchain.

Picture a day spent doing some work in a café. Anticipating a full day's stay, you open a tab and prepay some money instead of paying each time you order something. When you're ready to leave at the end of the day, you and the owner review the tab to settle the final bill. If you paid more money up front than the total amount of your final bill, you will receive back whatever amount you did not spend.

Now, envision thousands of people doing the same thing simultaneously and allowing others to use their tabs to connect with more people. That's the Lightning Network!

With Lightning, you can make payments to anyone on the network, not just the person you share a direct tab with. Your payment can navigate through the network until it reaches its destination, even if you don't have an open channel with the recipient.

Let’s take a look at the difference between on-chain transactions (the type we discussed in Chapter 7) and off-chain transactions (Lightning Network).

On-Chain Transactions:

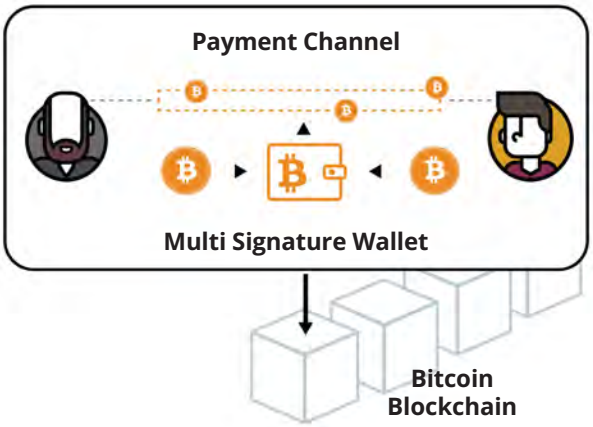
These are transactions that happen directly on the Bitcoin blockchain. They take about 10 minutes to confirm, and the fees depend on the size of the transaction in bytes. They are more secure but slower.

Lightning Network: Using Bitcoin in Your Daily Life

Off-Chain Transactions (Lightning Network):

These transactions happen on a separate network built on top of the Bitcoin blockchain. They are settled faster and with lower fees.

They are commonly used where regulations and laws support their adoption and where features like the speed and cost of transactions are more important. Compared to on-chain transactions, they are less secure.



Payment Network	Bitcoin Network	Lighting Network
Definition	A decentralized digital network that uses cryptography to secure financial transactions.	A second layer payment protocol that operates on top of the Bitcoin blockchain, enabling faster and cheaper transactions.
Advantages	Decentralized and secure. No charge-backs or fraud. Can be used anonymously. Global acceptance.	Faster and cheaper transactions. Increased scalability. Off-chain transactions do not clog the blockchain.
Disadvantages	Slow transaction times. High fees for certain types of transactions. Complex for beginners.	Requires trust in the channel operators. Still experimental and not widely adopted. Requires on-chain transaction to open and close channels.

8.2 Different Types of Lightning Wallets

A Lightning wallet is a bit different than a Bitcoin wallet, though it performs the same function: receiving and sending bitcoins. The difference is that a Lightning wallet allows you to send bitcoins on the Lightning Network, which itself is a second layer on top of the Bitcoin network.

Just as we saw in the previous chapter with Bitcoin wallets, Lightning wallets have different characteristics that need to be considered before choosing one.

8.2.1 Self-Custodial vs. Custodial Wallets

Lightning wallets can be broken down into very specific categories, but for the sake of simplicity, we'll divide them into two: self-custodial and custodial.

Just like Bitcoin wallets, a self-custodial Lightning wallet is one where you control the keys to the wallet, whereas a custodial Lightning wallet is one where someone else controls the keys.

When using a custodial wallet, you're only given access to the wallet but you depend on someone else for permission to use your money; you're giving up ownership of your money for convenience.

This can be acceptable for small amounts, although it's recommended to use a self-custodial wallet once you have an understanding of the technology.

For what follows, we'll be talking about self-custodial Lightning wallets only.

8.2.2 Open Source vs. Closed Source

Just like with the Bitcoin wallets we saw in the previous chapter, Lightning wallets can be open-source or closed source. Always use open-source wallets as they are completely open for review and vetted by the community.

An open-source application also means that anyone can contribute to the improvement of the software, making it a better choice for users.

8.3 Setting up a Bitcoin Lightning Wallet

Setting up a self-custodial Bitcoin Lightning wallet is the same as setting up a self-custodial on-chain Bitcoin wallet.

Lightning Network: Using Bitcoin in Your Daily Life

Class Exercise — Option 1: Download a new self-custodial lightning wallet

How to Create and Use a Bitcoin Lightning Wallet

1. Search for the app in the App Store (iOS) or Google Play Store (Android).

2. Open the app and type in your 12- or 24-word recovery phrase (sometimes called a seed phrase). **Be sure to write it down and keep this in a safe place!** This recovery phrase allows you to recover full access to your funds if needed.

Remember that if you lose or forget this sequence of words, you will not be able to access your bitcoins if you lose access to your wallet.

3. You must then confirm that you have actually saved your recovery or seed phrase. To do this, you must enter, in the same order, the words of your seed phrase.

4. As an additional measure of security, some wallets allow you to choose a secure password. Your private key and first Bitcoin address are automatically created for you by your wallet.

5. Generate a Lightning invoice, address, or QR code to receive bitcoins. Transfer bitcoins to your wallet. With a self-custodial wallet, you cannot always buy bitcoins directly with fiat, so you might need to purchase and transfer them from an exchange first.

Your Seed Phrase

Your seed phrase is used to generate and recover your account.

1 Issue	2 Flame	3 Sample	4 Lyrics	5 Find
6 Vault	7 Scissors	8 Banner	9 Cute	10 Damage
11 Civil	12 Goat			

Please save these 12 words on a piece of paper. The order is important. This seed will allow you to recover your account.

*Note: If you are using a custodial wallet, you will not need to follow some of the steps in section 8.3. Using a custodial wallet comes with risk, as you will not be in control of your private key, which means you will not be in control of the money you keep in your wallet.

Now that we have set up our Bitcoin Lightning wallet, let's look at receiving and sending Lightning transactions and how they differ from the on-chain transactions we sent in Chapter 7.

8.4 Sending and Receiving Lightning Transactions

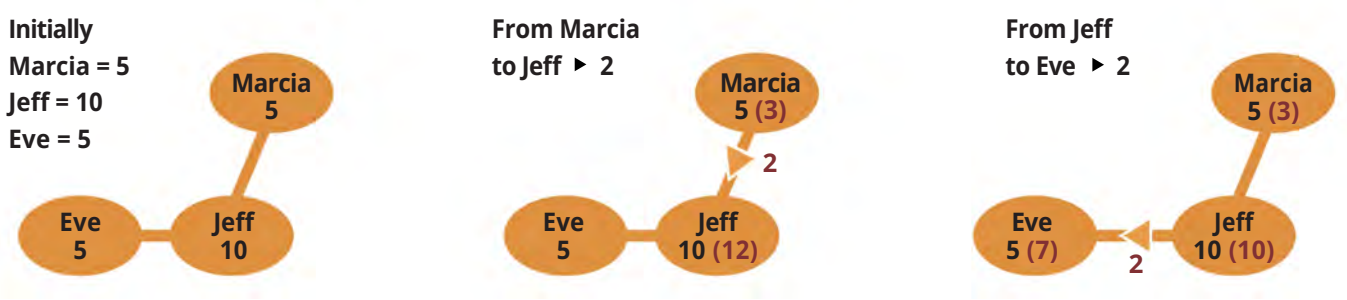
With a Lightning wallet, using Bitcoin is fast, cheap, and private, making transactions between two people easy. You can quickly send and receive bitcoins for everyday things like buying coffee or shopping.

Let's look at a few examples of the Lightning Network in action.

Example 1:

Below, both Marcia and Eve have 5 units of currency each. Marcia wants to send 2 of her units to Eve, so she sends 2 units to Jeff. Jeff then passes on the 2 units to Eve, who now has 7 units. Marcia now has 3 units. And that's it! The transaction is done.

The key point here is that Marcia and Eve don't have to go through a bank or other intermediary to make the transaction happen.



Jeff acts as an intermediary or a "trusted third party" in this scenario, where Marcia and Eve do not trust each other directly. Jeff receives the 2 units from Marcia and then passes it on to Eve, thus completing the transaction. By using Jeff as an intermediary, Marcia and Eve can complete the transaction without the need for a bank or other centralized institution, which can make the transaction faster, cheaper, and more secure. Jeff is a key element in this peer-to-peer transaction process.

As a node operator in a Lightning Network transaction, Jeff benefits in several ways:

1 Transaction Fees

Jeff earns a small fee for each transaction that passes through his node, which compensates him for the time and effort he puts into maintaining and running his node.

2 Network Participation

By running a Lightning node, Jeff is participating in the network and helping to increase its decentralization, security, and stability. This can increase Jeff's reputation and credibility as a reliable node operator, making him a more attractive intermediary for future transactions.

Lightning Network: Using Bitcoin in Your Daily Life

3 Network Growth

As the Lightning Network grows and more people use it, the number of transactions passing through Jeff's node is likely to increase, which can result in increased income from transaction fees.

4 Increased Network Security

Jeff's role as an intermediary helps to increase the network's security by adding an additional layer of protection between Marcia and Eve. This can increase the users' confidence in the network, making it more attractive to new users and helping to drive growth. Overall, being a node operator in the Lightning Network can provide Jeff with a steady source of income, as well as the opportunity to contribute to the network's growth and development.

In summary, **on-chain transactions are slower but more secure, while off-chain (Lightning Network) ones are faster but less secure.** You should consider the trade-off between security and speed depending on your needs.

Example 2:

Mina has a serious love for McDonald's; she goes there for breakfast, lunch, and dinner every day! But with so many different payment options available, she's not sure which one is the best choice. Luckily, she's learned a little bit about Bitcoin and the Lightning Network. After comparing the tables below, Mina has no doubt that using a Lightning payment method is the way to go.

The Lightning Network vs. The Traditional Banking System

Benefits	Lightning	Traditional Banking System
Speed	Fast	Slow
Transparency	Transparent	Opaque
Security	Secure	Vulnerable
Transaction Fees	Low	High
Financial Inclusion	High	Limited

Benefits	Lightning	Traditional Banking System
Scalability	High	Low
Privacy	High	Moderate
Interoperability	High	Low
Legal Compliance	Moderate	High
Cost-Effectiveness	High	Moderate

Visa, Inc.

On average 1,700 transactions per second.

Capacity of 65,000 transactions per second.

Bitcoin On-Chain

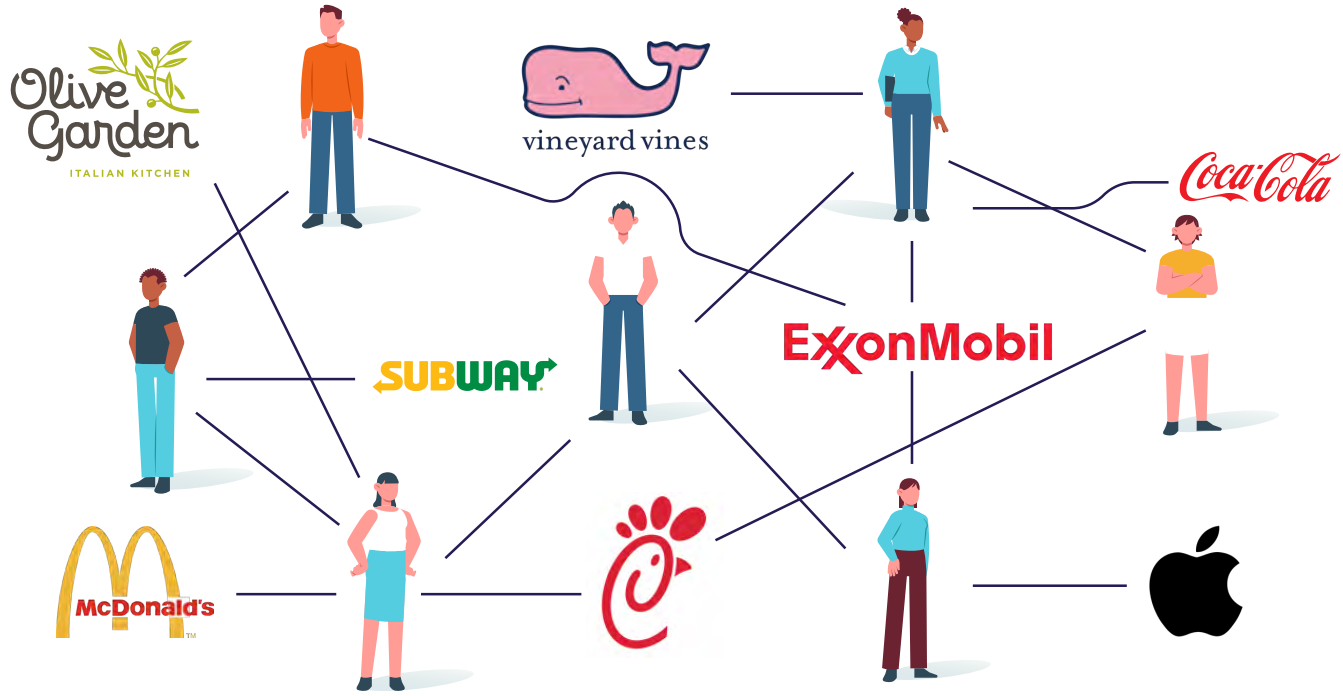
Capacity of 7 transactions per second.

Bitcoin Lightning Network

Millions of transactions per second.

Mina is also a fan of fast, secure, and cost-effective transactions, so she decided to use Lightning for her purchases at McDonald's. With Lightning, she can enjoy her meals even more knowing that her payments are processed instantly, securely, and with low fees. Plus, since the Lightning Network provides financial inclusion, Mina can now pay for her meals even if she is in a remote area in El Salvador.

To get started with Lightning, Mina first downloads a Lightning wallet on her phone. She then funds her wallet by sending some bitcoins from her regular Bitcoin wallet to her new Lightning wallet. This process is called "funding the wallet" or "funding a payment channel." Mina can fund her wallet with any amount of bitcoins she is comfortable with, but it's important to note that the amount of bitcoins she locks in her Lightning wallet cannot be used in her on-chain transactions.



Once her Lightning wallet is funded, she can use it to make payments to McDonald's.

McDonald's has a Lightning node, so Mina can open a payment channel with them by sending some of her bitcoins from her Lightning wallet to a specific address provided by McDonald's. This moves her bitcoins from the Bitcoin blockchain to an off-chain transaction on the Lightning Network.

With the payment channel open, Mina can now make purchases at McDonald's without having to open a new channel or pay high fees each time. The channel stays open as long as both Mina and McDonald's want to use it. For example, if Mina buys a hamburger for 0.0005 bitcoins, the channel tracks that Mina now has 0.9995 bitcoins. And if she buys a milkshake for 0.0003 bitcoins the next day, the channel tracks that Mina now has 0.9992 bitcoins.

Lightning Network: Using Bitcoin in Your Daily Life

When Mina decides she wants to use her bitcoin balance for something else, she closes the channel by broadcasting a closing transaction to the Bitcoin blockchain. This is done by initiating a closing transaction in her Lightning wallet, and the transaction contains the final balance of the channel agreed to by both parties. The transaction is then broadcast to the Bitcoin blockchain and confirmed by a miner. Once the transaction is confirmed, the channel is closed, and the remaining bitcoins in the channel will be returned back to Mina and McDonald's.

It's important to note that closing a channel can take some time to be confirmed on the blockchain. During this waiting period, the funds are still locked in the channel and cannot be used for on-chain transactions. Mina will receive a notification once the closing transaction is confirmed.

Now that we have set up our Lightning wallet and read about how to use the Lightning Network to send transactions, we are going to play a game where we send satoshis (the smallest unit of bitcoin) to other students in the class over the Lightning Network.

This is a map of the entire world. With the Lightning Network, you can send satoshis to any user with a Bitcoin Lightning wallet. The payment will arrive in a few seconds and will only cost a few cents.

Check it out for yourself:

Activity: Class Exercise - Lightning Wallet Relay Race

1. First, you will need to download a Lightning wallet onto your phone or computer.
2. Follow the instructions for installing the wallet on your device in Section 8.3 of this chapter.
3. Once the wallet is installed, open it and follow the prompts to set it up. This may involve creating a new wallet or restoring an existing one and securing it with a password or other form of authentication.
4. Generate a Lightning invoice, address, or QR code to receive bitcoins.
5. When your wallet is set up and you are ready to receive satoshis, your teacher will give you and your group a starting amount of satoshis by sending them directly to your wallet.

A. Your group's goal is to pass the satoshis from one person's wallet to another using the Lightning Network until they reach the last person in the group.

B. To send satoshis to another person, open your wallet and follow the instructions for making a payment. You will need to provide the recipient's Lightning invoice or scan a QR code and enter the amount of satoshis you want to send.

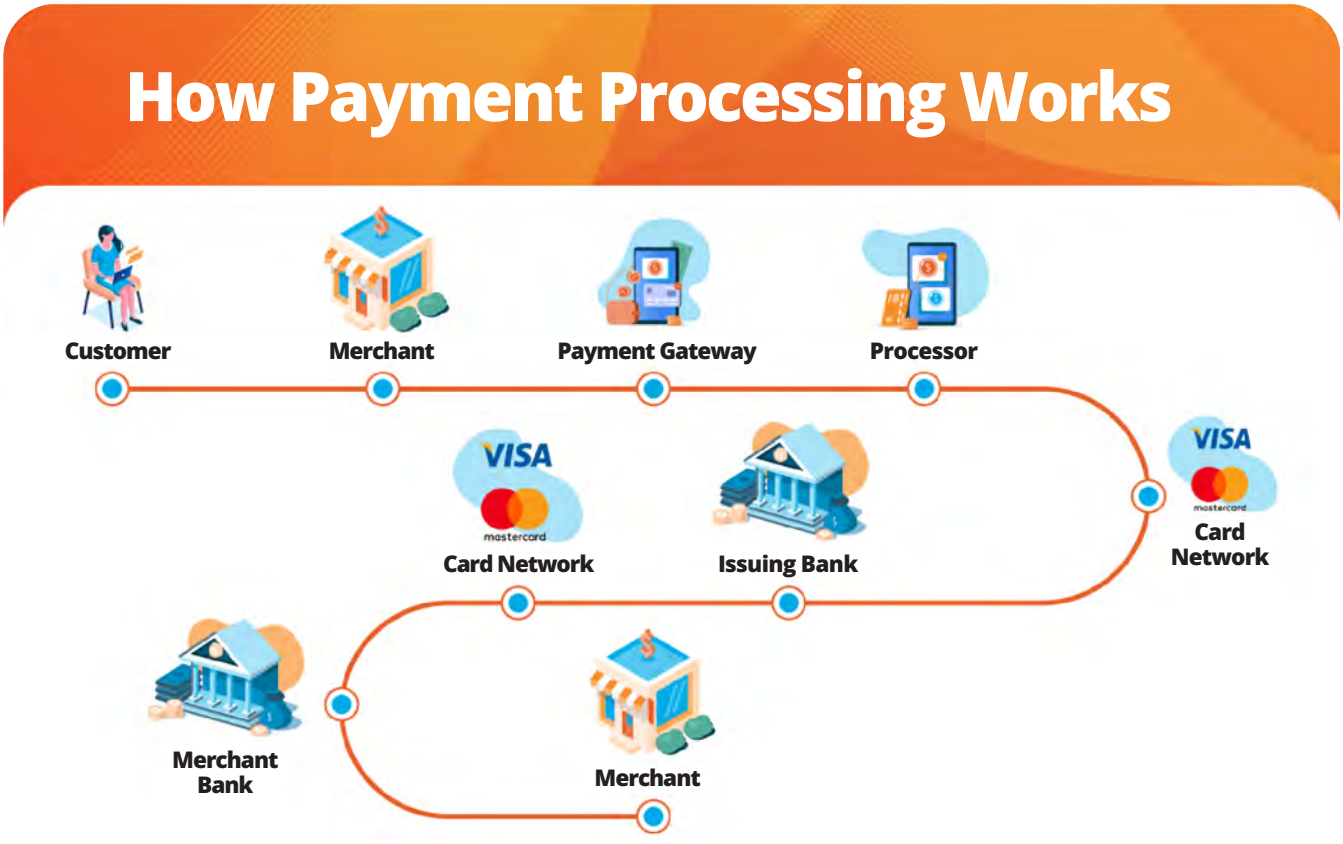
C. If your group is the first to successfully send the satoshis to the last person, you win! (And get to keep the sats).

Discuss any difficulties your group had with the activity. Was sending a transaction easy, fast, and inexpensive? Do you think the Lightning Network is easy to use and understand?

8.5 Buying Coffee and Groceries with Bitcoin

Have you ever wondered if you could use bitcoins to buy your daily cup of coffee or stock up on groceries? Turns out you can. There are many options, both online and in person, that let you pay with bitcoins. We'll explore some of those options and tools that will help you find local stores so you can spend bitcoins.

Even though paying with a credit card or an app can seem easy to understand for the person paying, the processing of the payment is actually very complex and involves many different parties.



When you buy things, there are many parties involved, and each party charges a fee. For store owners, these fees can be a lot — more than 3% of the price, which is a big amount for them.

And that's not to mention currency exchange fees!

Credit Card Processing Fees

$100	-$1.75	-$0.14	-$0.30	-$97.81
Customer Pays	Issuing Bank	Card Network Processors	Payment Processors	Goes to Merchant

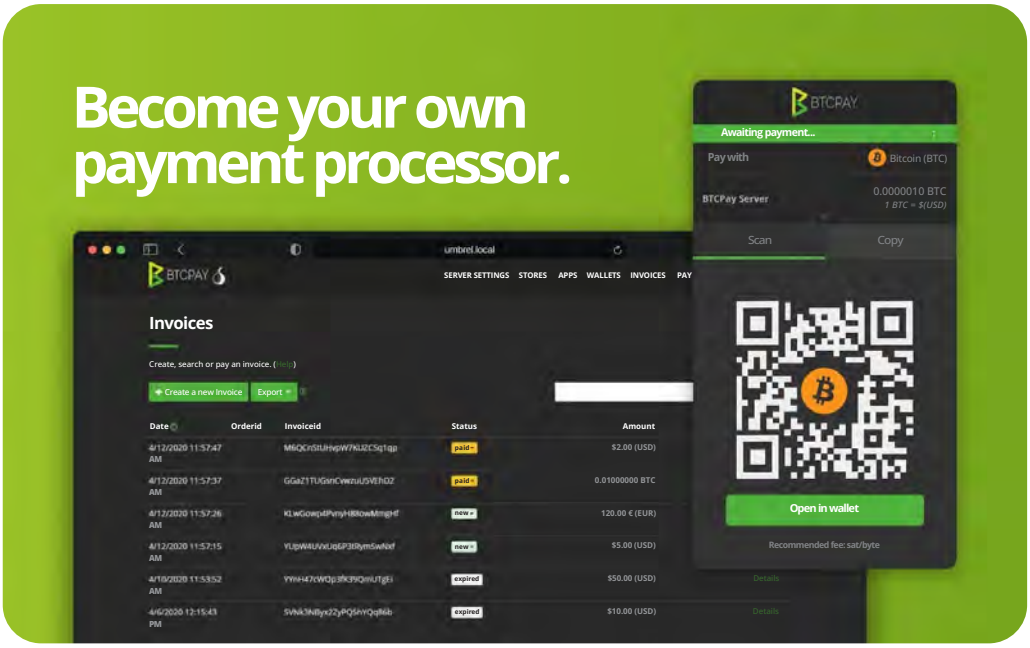
With Bitcoin and the Lightning Network, businesses can receive instant payments from all over the world via an open, secure, internet-native, borderless, and censorship-resistant monetary system.

Next, we will look at a few ways merchants can easily accept payments in bitcoins.

8.5.1 Online: Payment Plugins — Ecommerce

BTCPay Server is an open-source payment processor that allows merchants to accept payments in bitcoins with little technical knowledge. It's completely free and doesn't charge any commission.

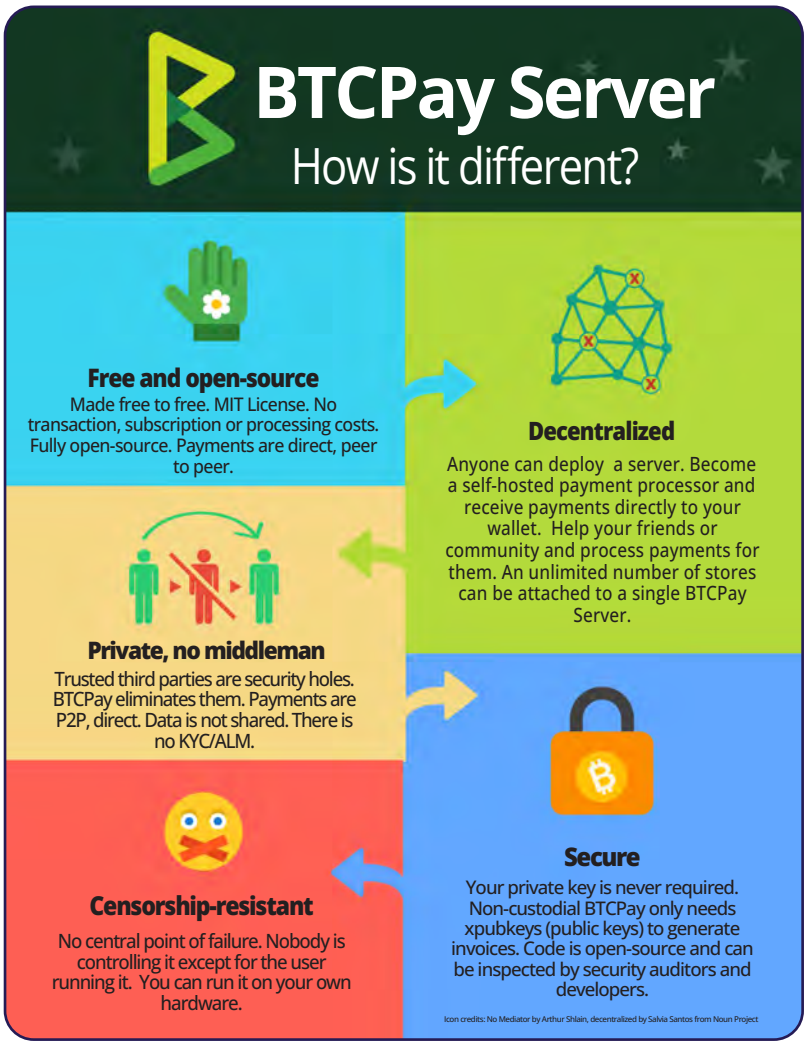
Online businesses can integrate BTCPay Server seamlessly by adding the BTCPay plugin to their website.



Lightning Network: Using Bitcoin in Your Daily Life

Because BTCPay Server is an open-source project, not a company, you can contribute to the project once you learn more about it and computer programming.

Check out BTCPayServer at https://btcpayserver.org/ for more information on how to use this payment system for your in-person or online business.

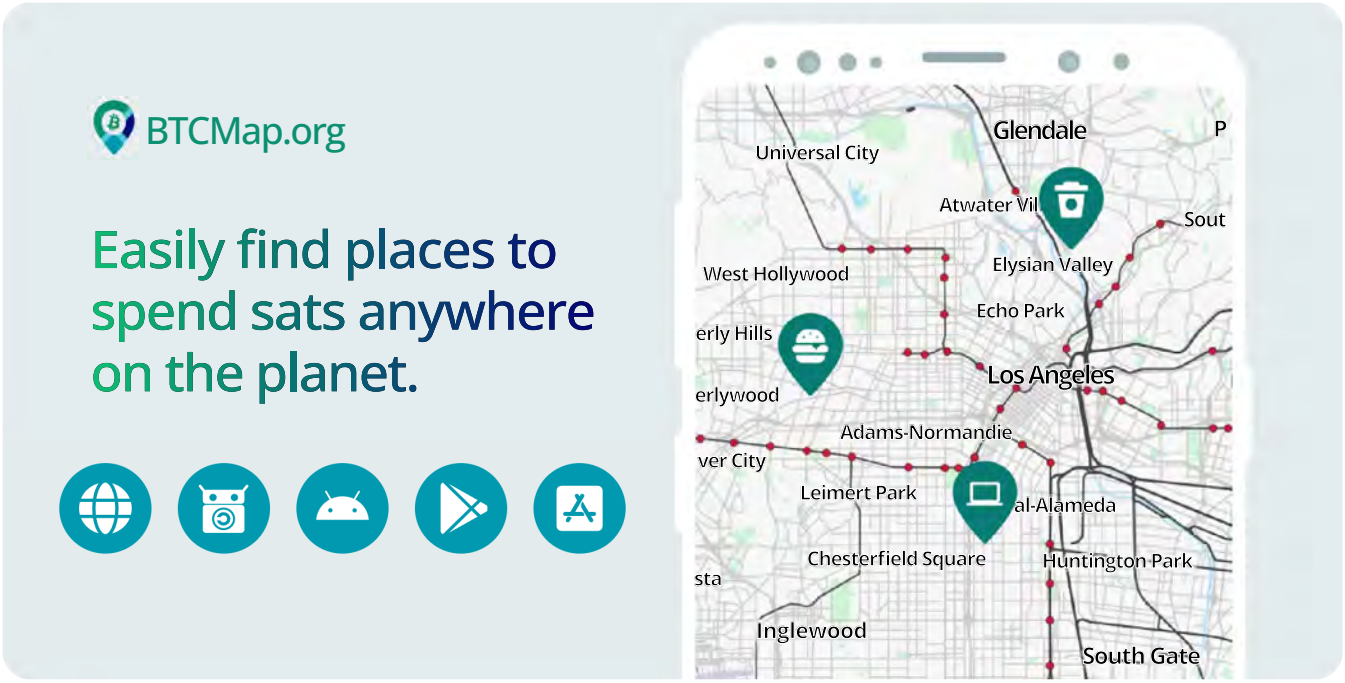


8.5.2 In-Person: Find a Merchant in Your Area

Physical shops can also use BTCPay Server to accept payments, or they can simply download a Bitcoin wallet and accept Bitcoin payments directly from their phone.

To find a merchant that accepts Bitcoin in your area, go to BTCMap.org and search for your region.

BTCMap.org is an open-source map where merchants that accept Bitcoin can list their businesses. It's a powerful tool for people who wish to spend their bitcoins.



8.5.3 Transitional Tools: Vouchers, Gift Cards, and Payment Cards

To purchase products or services from businesses that do not yet accept Bitcoin, there is an intermediary tool you can use: gift cards.

Some businesses focus on buying and selling gift cards in exchange for bitcoins. That means you can acquire a gift card for the store you'd like to go to in exchange for bitcoins and then spend the gift card directly at the store.

Plane tickets, hotels, games, SIM cards... you can buy almost anything with bitcoins and gift cards!

8.5.4 Circular Economies and Bitcoin as a Medium of Exchange

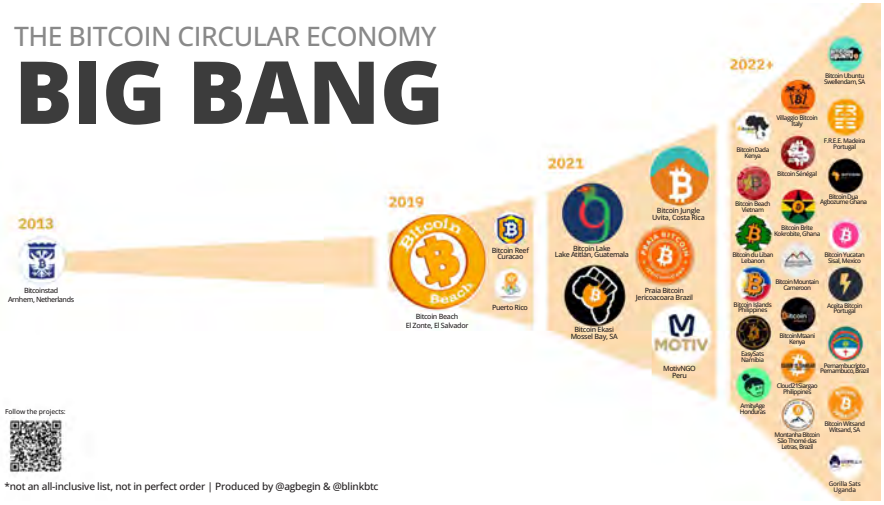
The concept of the circular economy comes from the idea of minimizing waste in an economy by reusing and recycling as many products and byproducts as possible.

Drawing from this concept, a Bitcoin circular economy is one where the transactions are made in bitcoins and where the money in the form of bitcoins stays and grows within the economy, benefitting its individuals and businesses.

Lightning Network: Using Bitcoin in Your Daily Life

The Lightning Network enables Bitcoin circular economies to flourish all around the world thanks to near-instant and low-fee bitcoin transactions.

The first Bitcoin circular economy ever created is located in Arnhem, Netherlands. It was created way before the Lightning Network existed, but back then, on-chain fees were really low!



The second one was Bitcoin Beach, located in El Zonte, El Salvador. It leveraged the power of the Lightning Network to provide the community, which was mostly unbanked, with instant digital payments directly with their smartphones!

Today, hundreds of circular economies are being created all around the world, powered by Bitcoin, the Lightning Network, and educational resources.

On BTCMap.org, you can also look for Bitcoin communities where you will meet other Bitcoin users and find businesses that accept Bitcoin. Some of our teachers and students have actually added businesses and circular economies to BTCmap.org, and once you are ready, you can too!

Resource: btcmap.org/communities

As we wrap up Chapter 8, you've gained insights into using Bitcoin in your daily life through the Lightning Network. The Lightning Network makes transactions quicker and more accessible, offering a preview of how Bitcoin will continue to change and evolve in layers.

In Chapter 9, we will investigate the technical side of Bitcoin. From cryptography to nodes, miners, and more, get ready to take a closer look at how Bitcoin really works.

Chapter #9

An Introduction to the Technical Side of Bitcoin

9.0 Introduction

Activity: Watch “How Bitcoin Works under the Hood”

9.1 Public and Private Keys: Security through Cryptography

9.1.1 Cryptography Public/Private Keys

9.1.2 Hashing Explanation

Activity: Generate SHA 256 Hash

9.2 The UTXO Model

9.3 Bitcoin Nodes and Miners

9.3.1 What Is a Bitcoin Node and How Do I Set One Up?

Activity: Watch Video on Bitcoin Nodes

9.3.2 What Is a Bitcoin Miner and How Does Mining Work?

9.4 What Is the Mempool?

Activity: Mempool

9.5 How Bitcoin Transactions Work from Start to Finish

Student Workbook

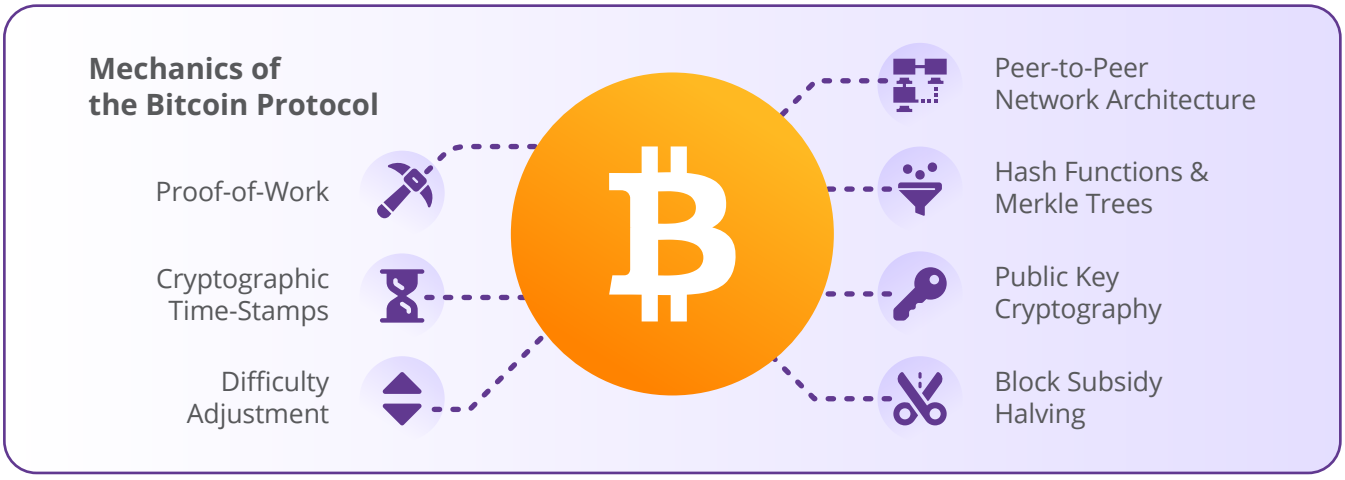
English Version | 2025

An Introduction to the Technical Side of Bitcoin

9.0 Introduction

> Bitcoin is not “unregulated”; it is regulated by algorithm instead of being regulated by government bureaucracies. Uncorrupted.
>
> **Andreas M. Antonopoulos**

In this chapter, we will take a closer look at the technology that enables the Bitcoin network to operate in a fully decentralized way. We will explain in simple terms what happens when you send a bitcoin transaction, how those transactions are processed, and what miners and nodes do in the Bitcoin network. We are going to cover some challenging and technical concepts in this chapter. One important thing to remember: many people don’t understand how the internet works, yet they are able to use it every day to send emails, contact friends on social media, and even pay their bills. Learning the technical side of how Bitcoin works is a long journey that not everyone may want to take, even if they decide to use it as money. While we do encourage you to keep learning about the technical aspects of Bitcoin, we will keep this chapter focused on basic key concepts.



If you want a deeper technical understanding of how Bitcoin works, we have included resources in the back of this workbook. You can also register on our website for the Bitcoin Diploma - Technical Edition to be notified when this more technical course is ready.

Let’s jump in by watching a video that shows how the Bitcoin network works.

Activity: Watch “How Bitcoin Works under the Hood”

As you saw in the video, the Bitcoin network is simply a ledger or record of transactions stored on multiple computers called nodes. The Bitcoin ledger is pseudonymous, meaning it doesn't have personal details, only transaction and address information. The ledger shows every bitcoin and its movements since the network started on January 3, 2009.

Next, we'll take a closer look at the technology that makes this system possible.

9.1 Public and Private Keys: Security through Cryptography

> What Bitcoin gives us is a hard promise: the program will execute exactly as specified.
>
> **Andreas M. Antonopoulos**

9.1.1 Cryptography Public/Private Keys

Cryptography is a way of keeping information secret by disguising it in code.

- Encryption is the process of taking information and transforming it in a special code, making it unreadable to anyone who does not have the correct decryption method. This is similar to locking a safe, where only the person with the correct key or combination can open it.

- Decryption, on the other hand, is the process of taking the encrypted information and making it readable again, like unlocking the safe and being able to read the information inside.

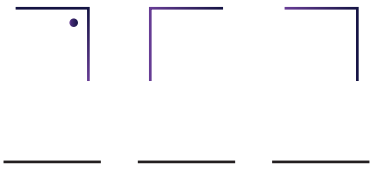
For instance, let's say John wants to send Arel a secret message that isn't meant for anyone else to read. They agree to use the Pigpen Cipher encryption method to disguise the message before sending it. Only those with the cipher can decrypt the message, making it unreadable to anyone else. Though this method is not considered secure today, it does illustrate the principle of private-key cryptography to send messages.

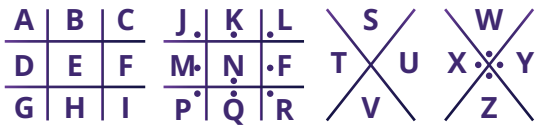
How to Solve

Pigpen Cipher

When solving the Pigpen Cipher, the player is given an encrypted message and a cipher. To decrypt the message, the player will find the symbol from the encrypted message on the cipher to find the decrypted letter.

- Example of an encrypted message:





So, how does cryptography work in bitcoin transactions?

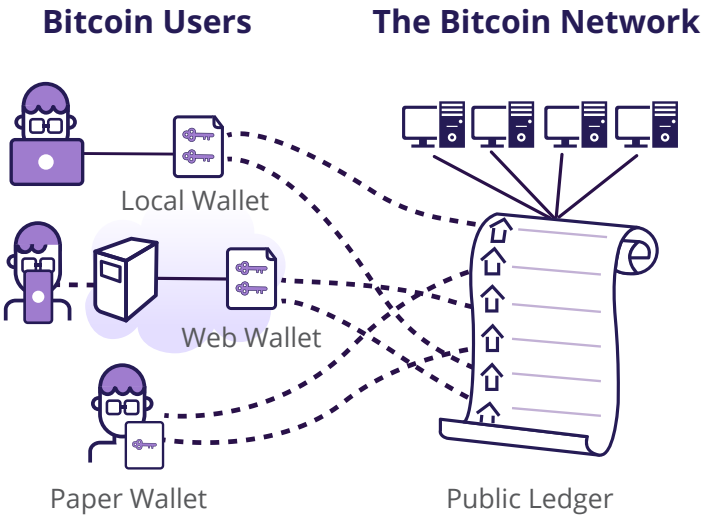
In traditional private-key cryptography, John and Arel would have to first share a secret key, like a password or the Pigpen Cipher. John would then use this key to encrypt his message before sending it to Arel. Arel, who also knows the secret key, would then use the same key to decrypt and read the message.

However, if someone else is in possession of the key and intercepts the message, they could decrypt it and read it.

An Introduction to the Technical Side of Bitcoin

Public key cryptography, the type used in bitcoin transactions, has solved this problem. With public key cryptography, John and Arel don't need to share a password or encryption method with each other. Instead, they each have two different keys: a **public key** (which is safe to share with anyone) and a **private key** (which should be kept private).

In this case, when John wants to send a message to Arel, he can use Arel's **public key** to encrypt his own message before sending it to Arel. When Arel receives the message, only he is able to decrypt it with his **private key**. Anybody else, even if they intercept the message, would not be able to read the message. The chances to steal the key are also much lower because even John and Arel don't need to share their private keys with each other.



So, the main advantage of public key cryptography over private is that it allows for secure communication without the need for the sender and receiver to first share a secret key (or another encryption method like Pigpen Cipher), which could be intercepted by a third party.

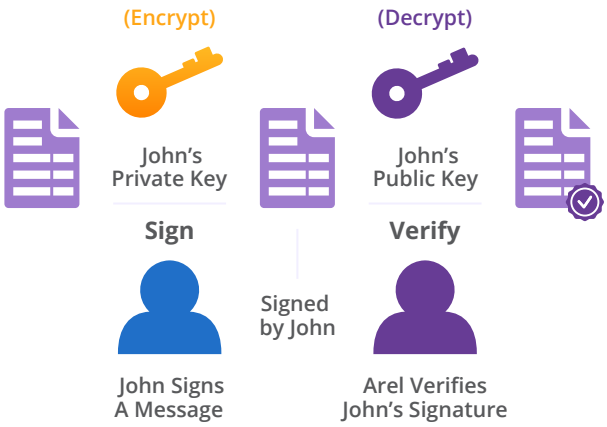
In Bitcoin, public key cryptography is not used to send encrypted messages. Instead, it is used to create unique **digital signatures** that make bitcoin transactions immutable. A **digital signature** is a way to prove a bitcoin transaction's authenticity, similar to when you write your signature on a physical document.

Public Key Cryptography (for every transaction between two users):

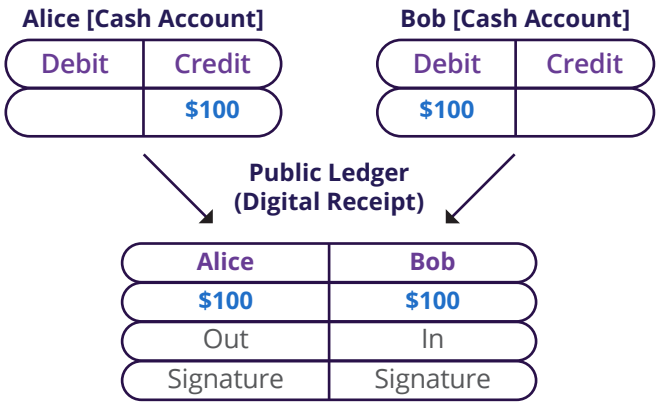
Each user has two keys: a **private key**, which is **kept secret**, and a **public key** that can be **shared with others.**

The **private key** serves as a form of identification and proof of ownership, confirming: **"This address belongs to me and I have control over it."**

Digital signatures are created to identify unique transactions.

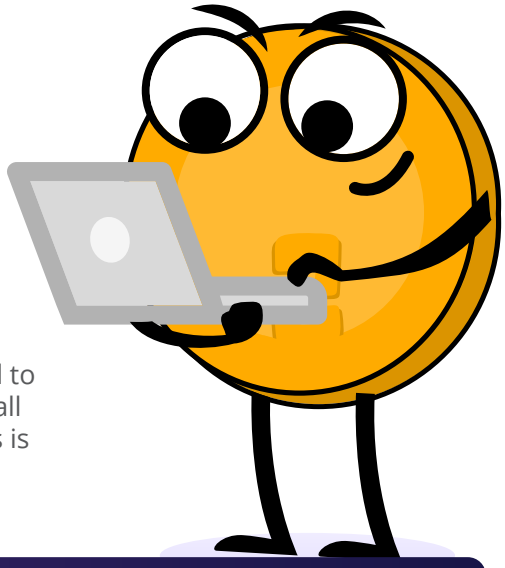


- Bitcoin transactions involve transferring a certain amount of bitcoins directly to another person's account.
- Encryption is used to ensure that only the real holder of the bitcoins has the control to send their money to someone else. It makes sure that the property is guarded against malicious actors.
- As an additional measure of protection, each transaction that you send in Bitcoin automatically gets a **UNIQUE signature**. This **unique signature** is empowered by tamper-proof technology that helps the network verify that the real owner of the bitcoins, and not someone else, has sent them.



How this works in a real bitcoin transaction in simple terms:

1. **Creating the Transaction:**
   A user initiates a bitcoin transaction by specifying details such as the recipient's address and the amount of bitcoins to be sent.
2. **Digital Signature Generation:**
   The sender generates a unique **digital signature** using their **private key**. This signature is a unique cryptographic code that verifies the transaction's authenticity.
3. **Broadcasting the Transaction:**
   The signed transaction is broadcasted to the Bitcoin network, indicating the intent to transfer ownership of bitcoins from the sender to the recipient.
4. **Verification on the Network:**
   Nodes on the Bitcoin network receive the transaction and use the recipient's **public key** to decrypt and verify the integrity of the transaction. Simultaneously, they use the sender's **public key** to verify the **digital signature**.
5. **Confirmation on the Bitcoin Network:**
   If the verification is successful, the transaction will be added to the ledger, which serves as a secure, transparent record of all transactions. Once confirmed, the ownership of the bitcoins is officially transferred from the sender to the recipient.



In summary, the digital signature, created with the sender's private key, serves as cryptographic proof of authenticity and ownership, allowing Bitcoin's decentralized network to validate and record the transaction on the ledger.

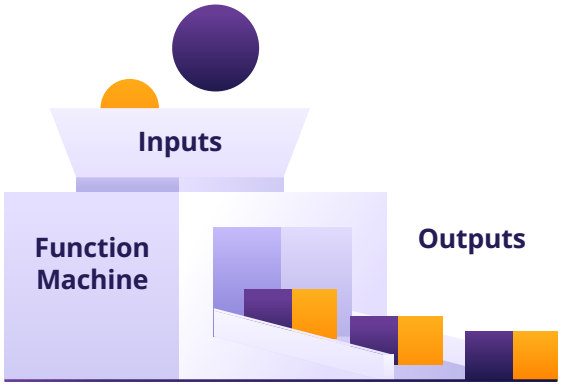
An Introduction to the Technical Side of Bitcoin

9.1.2 Hashing Explanation

Please don't be intimidated by the technical terms and mathematical concepts ahead. We understand that not everyone is crazy about math, but you might surprise yourself and see that even the most complex ideas can be grasped with a little bit of effort.

What Is a function?

A **function** is like a machine that takes some information and turns it into something new. The information you give the function is called the **input.** The new information the function creates is called the **output.** Functions help computers do tasks and solve problems.



Think of it like a recipe for making a salad. The recipe (or function) tells you what ingredients to use and how to mix them together to make the salad. You can put different ingredients in, but the recipe will always give you the salad as the output. Functions can be used to help make things easier and more efficient.

This recipe is a function that takes the ingredients as the **input** and generates the tossed salad as the **output**.

In Bitcoin, functions are utilized to execute transactions. We already know that bitcoin transactions are essentially transfers of value (money) from one address to another. To perform a transaction, a number of cryptographic functions are used to validate the transaction and update the state of Bitcoin's ledger.

The functions used in a bitcoin transaction include verifying the authenticity of the transaction inputs, checking that the sender has sufficient funds, and updating the balances of the relevant addresses. Once a transaction is verified and added to a block in the ledger, it becomes part of the permanent record of all transactions on the network.

What Is a One-Way Function?

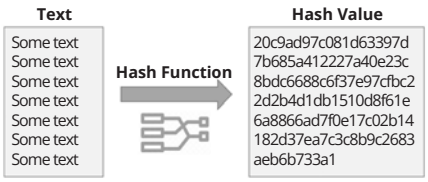
A one-way function uses a set of instructions to process information and turns it into something new, like a smoothie recipe turns ingredients into a new drink. But, just as you can't un-blend a smoothie to get the original ingredients back, you can't reverse the one-way function to get the original information back.

Public-key cryptography, of which the **public key** is a part relies on the use of one-way functions, which make it difficult to determine the **private key** from the **public key**. In theory, it is not exactly "impossible" to find the **private key** from the **public key**, but it is extremely difficult to do so and would take an inordinate amount of time and computational power to do so. Finding a **private key** from a **public key** in Bitcoin is like trying to find a needle in a haystack as large as a football field. The needle represents the **private key** and the haystack represents all the possible **private keys**. In the same way, one-way functions are designed to be irreversible and cannot be decrypted.

What is a Hash Function?

Hashing is like a fingerprint for digital data. It is the process of taking a digital message and turning it into a fixed length code, which serves as a unique identifier.

Just like a fingerprint can identify a person, a hash can identify a digital message. Hashes are used in many applications, including bitcoin transactions.



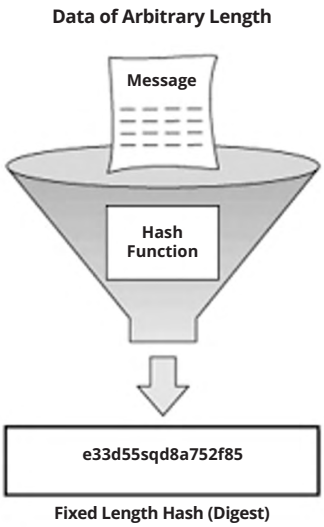
How Hashing Is Used in Bitcoin Transactions

In Bitcoin, every transaction is hashed before it is added to a block in the ledger. The hash acts as a signature for the transaction, verifying that the transaction is valid and has not been tampered with. If someone tries to change even a single letter in the transaction, the hash will be completely different, alerting others to the change.

The Role of Hashing in Providing Security

Hashing is essential to the security of the Bitcoin network. By using hashes to identify transactions, the network can detect any attempt to change or manipulate a transaction. This helps to prevent fraud and ensure that all transactions are recorded accurately on the ledger.

A hash function is a type of one-way function that takes an input (referred to as the "message" or "data") and converts it into a numerical representation referred to as a "hash." The **output** hash is unique to the input data, so even a small change in the **input** data results in a completely different hash.



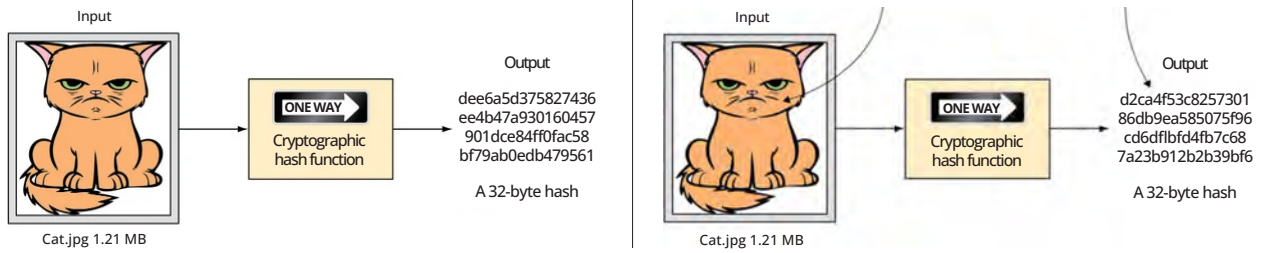
A hash function is like a secret code machine. It takes in a **message** and turns it into a code.

An Introduction to the Technical Side of Bitcoin

The code always looks the same for the same message. If you change the message even a little, the code will be completely different. This helps computers remember things and check if anything has been changed.

Instantly generate a SHA256 hash of any string or input value. Hash functions are used as one-way methods.

Activity - Generate SHA 256 Hash →



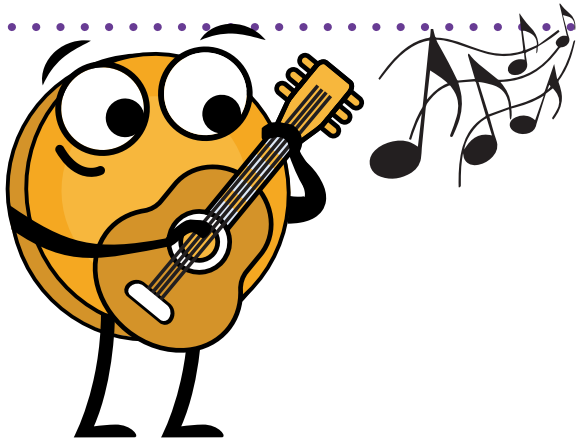
The **output**, or hash, is always the same length, no matter how long the original information was.

Bitcoin uses a few specific types of hash function called **SHA-256** and **RIPEMD160.** A few examples are below:

- Notice that a small change in the second input changes the output completely when compared to the first one.
- The third input is a huge file yet the output is still the same fixed length as the other two.

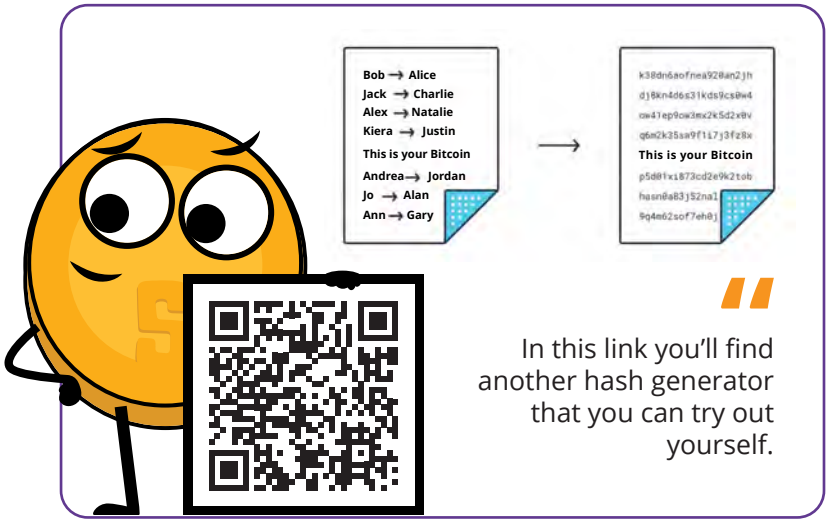
- SHA256 hash of the string ***hello world***
  B94d27b9934d3e08a52e52d7da7dabfac484efe37a5380ee9088f7ace2efcde9
- SHA256 hash of the string **hello world.**
  7ddb227315f423250fc67f3be69c544628dffe41752af91c50ae0a9c49faeb87
- SHA256 hash of the downloadable iso file **Ubuntu 18.10**
  7b9f670c749f797a0f7481d619ce8807edac052c97e1a0df3b130c95efae4765

Hashing can also be thought of as a musical score that captures the essence of a piece of music. Just as a musical score is a unique representation of a tune, a hash value is a unique representation of a piece of data. By comparing the score of a piece of music with the actual performance, a musician can determine if the performance is accurate. Similarly, by comparing the hash value of received data with the original hash value, one can determine if the data has been altered during transmission.



Just as a slight deviation in a musical performance can cause it to sound different, even the slightest change to the original data will result in a different hash value. This makes hashing a powerful tool for ensuring the integrity and authenticity of a bitcoin transaction.

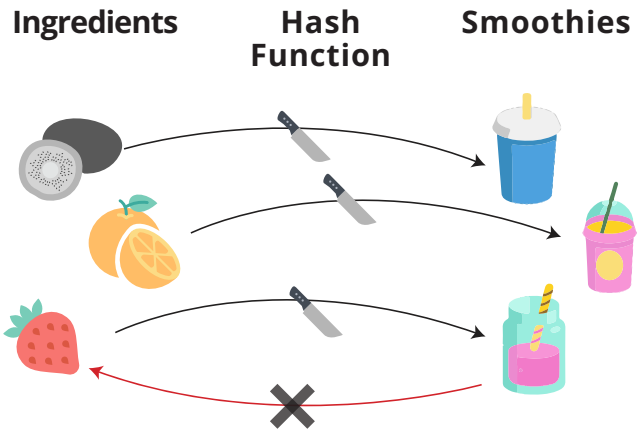
The process of encoding the **public key** through hashing is used to improve the security of information by converting it into a fixed-length, unreadable format. Bitcoin uses the SHA-256 and Ripemd-160 algorithms to produce public addresses. The resulting output serves as a unique identifier for the **public key** and helps to ensure the integrity and security of transactions stored in the ledger. By encrypting the information in this way, it becomes more difficult for unauthorized individuals to access and manipulate the data.



In this link you'll find another hash generator that you can try out yourself.

Hashing

A hash function takes any input, and produces a fixed-length output (hash).



- **Deterministic.**
  The same ingredients always yield the same smoothie.
- **Pre-Image Resistance.**
  You can't glue together a strawberry when given a smoothie.
- **Correlation Resistance.**
  Changing the ingredients a little results in a completely different smoothie.
- **Collision Resistance.**
  It's hard to find different ingredients for a smoothie that result in the exact same one.
- **Speed & Verifiablility.**
  Throw fruit into the mixer. It's fast and what comes out for sure is a smoothie.

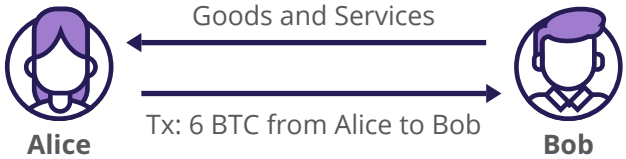
9.2 The UTXO Model

UTXO - Unspent Transaction Output

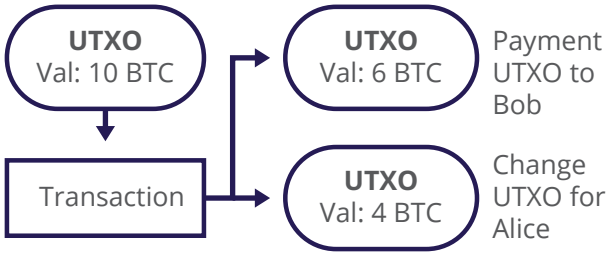
An Introduction to the Technical Side of Bitcoin

What Are UTXOs?

In Bitcoin, transactions work like breaking a bigger piece of gold into smaller pieces and sending these smaller pieces both to others and to yourself.



You can think of UTXOs as different sizes and pieces of bitcoin or differently denominated bills in your wallet. When you spend a UTXO, it is recreated into a new UTXO for the receiver, and whatever is left over is sent back to you in a different, new UTXO known as the "change UTXO." This is much like using a $10 bill to buy two cups of coffee for $6. The coffee shop keeps the $6 piece and hands you $4 in change.

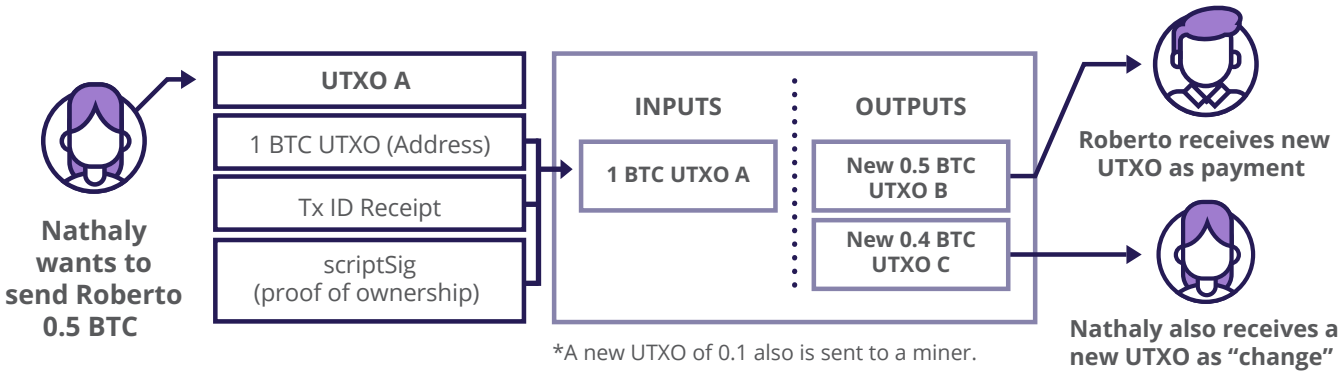


When sending bitcoins, you always send the entire amount of one (or more) of your UTXOs in your Bitcoin wallet. What happens? You send a piece to the recipient, and you receive the remaining amount back as change to one of your new Bitcoin addresses. The change you receive is called an unspent transaction output, or UTXO, and can be used as an input for a new future transaction.

The balance of your Bitcoin wallet is the sum of all your different UTXOs. So, the sum of your UTXOs is the sum of the amount of bitcoins you own.

It is important to note that you should not make others aware of your UTXOs because when someone knows them, they can track your bitcoin transactions in the network and will ultimately know how much money you own.

In conclusion, each time you make a transaction, you use one or more of your existing UTXOs to spend bitcoins and new UTXOs are created (for both you as the recipient).



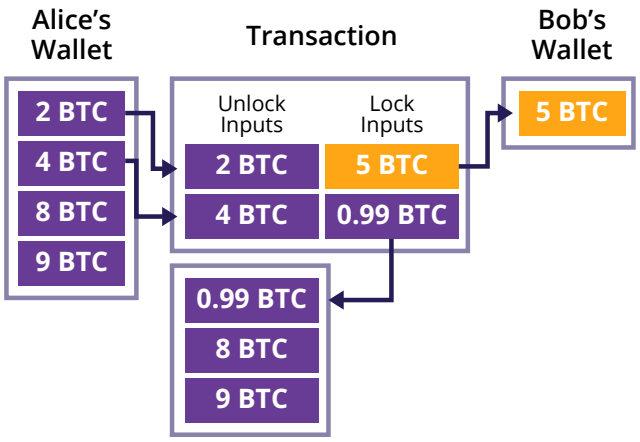
When a transaction is made, the amount of bitcoins sent is divided into multiple outputs, each of which is associated with a new Bitcoin address (a new UTXO).

When sending bitcoins to someone, you will use one or more UTXOs as the source of the funds (input). These UTXOs will be combined, if necessary, to create new outputs that belong to both the recipient of the transaction and yourself. These new outputs, or UTXOs, will become the recipient's property and your property. These UTXOs can then be used as the source of funds in other future transactions. This chain of UTXOs creates a transparent, traceable history of all bitcoin transactions on Bitcoin's ledger, starting from the very first block (January 3rd, 2009).

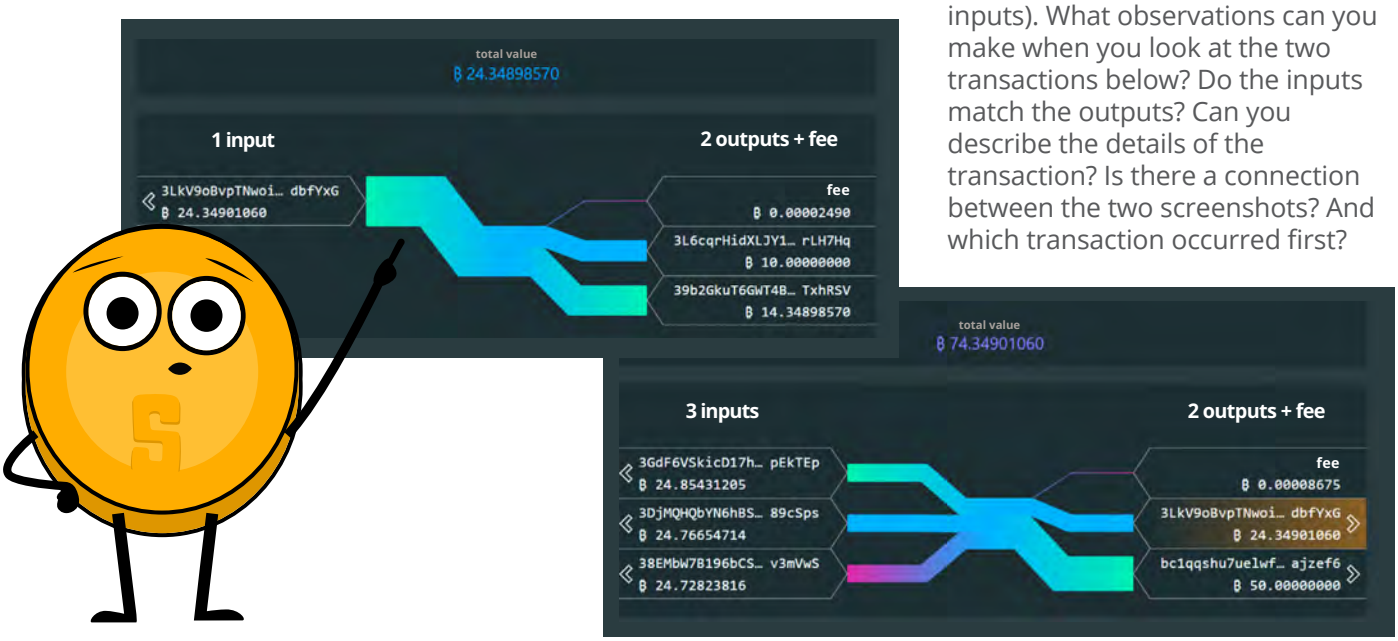
An example to illustrate how this works: if you want to send two bitcoins but you only have a UTXO worth five bitcoins, the difference of three bitcoins is sent back to you as "change". This change is a new UTXO for you, and you can spend that new UTXO in a future transaction.

Another example:

1. Alice wants to send Bob five bitcoins.
2. She combines six bitcoins from two of her UTXOs
3. From these UTXOs, she sends five bitcoins to Bob, gets 0.99 bitcoins as change back to herself, pays a 0.01 bitcoin transaction fee.
4. After confirmation, the transaction is added to Bitcoin's ledger, updating all the nodes that have a copy of the ledger.



If Alice attempts to use one of her already spent outputs to make another transaction, it will automatically be rejected by the nodes. This is because the nodes maintain a copy of Bitcoin's ledger (and all its transactions), so they can easily check the balance of Alice's UTXOs and verify that the transaction is not valid.



Below is an actual screenshot of a real transaction where there is only one input. However, the starting balance could, in another case, be the sum of multiple UTXOs (multiple inputs). What observations can you make when you look at the two transactions below? Do the inputs match the outputs? Can you describe the details of the transaction? Is there a connection between the two screenshots? And which transaction occurred first?

An Introduction to the Technical Side of Bitcoin

9.3 A Closer Look at Bitcoin Nodes and Miners

In this section, we'll take a more detailed look at two very important parts (and participants) of the Bitcoin network that were first introduced in Chapter 6. We'll look at:

1. **Bitcoin Nodes:**

   Gatekeepers of validation whose main job is to keep a copy of Bitcoin's ledger, making sure that all transactions are valid, and everyone follows the same rules.

   By spreading out this job among many people worldwide, Bitcoin stays strong against potential problems. These nodes help keep the system trustworthy and true to its decentralized idea, where no one person or group has too much power.

2. **Bitcoin Miners:**

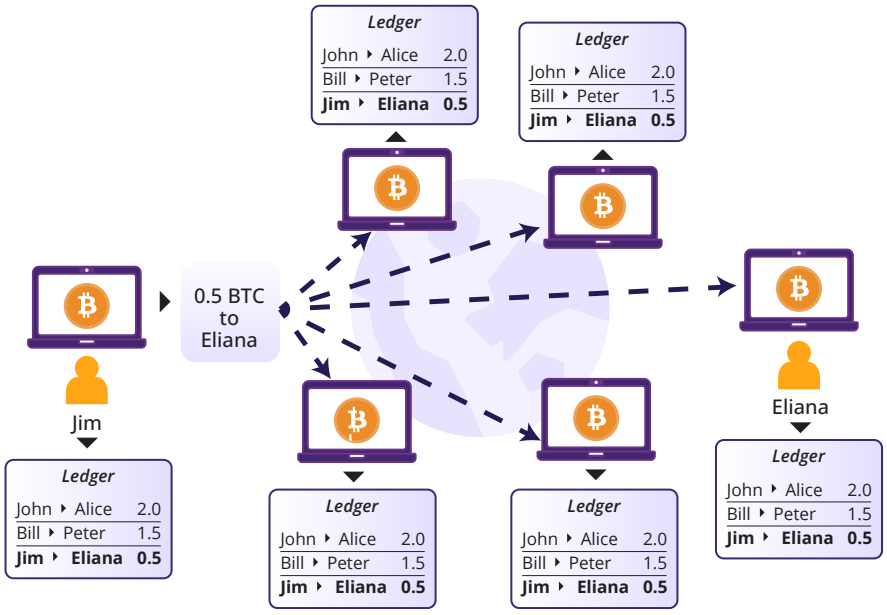
   Architects of security that use powerful computers and electricity to check and confirm transactions, making sure everything is secure. This work helps make the ledger, or blockchain, resistant to any bad actors trying to mess things up.

Together, Bitcoin nodes and miners work as a team to maintain a decentralized, secure, and strong system - a new way of handling money that people all around the world can rely on. Let's explore these roles in more detail to understand how they contribute to the innovative Bitcoin system.

9.3.1 What Is a Bitcoin Node and How Do I Set One Up?

A Bitcoin node may sound technical, but it is just a piece of software that runs a copy of the Bitcoin ledger. When you run your own Bitcoin node, you gain a voice in shaping the rules of the Bitcoin network.

Imagine this: if a group of people attempts to change how Bitcoin functions, say by altering the total supply of bitcoins, you have a say. You can choose not to change your node to the new system, which is like voting to enforce the rules of the network you support.



Let's imagine a Bitcoin node as a digital traffic cop with some essential tasks:

1. **Gatekeepers of Validation:**
A Bitcoin node keeps a digital copy of the blockchain, which is like a shared ledger of all bitcoin transactions. Many nodes around the world hold this same record.

2. **Communication Hub:**
Nodes connect with each other, creating a vast communication network. They share information, especially transactions waiting to be added to the blockchain, stored in a digital waiting room called “mempool."

3. **Quality Checker:**
Every addition to the blockchain undergoes scrutiny. Nodes ensure that transactions are valid, rejecting any that don't follow the rules of the Bitcoin network.

4. **Blockchain Informant:**
Other software, like wallets, can ask a node for information about the blockchain, such as bitcoin balances. Nodes serve as information hubs.

5. **New Node Welcomer:**
When a new node wants to join, existing nodes generously provide a copy of the blockchain. The new node independently checks the validity of each transaction, emphasizing a trustless system.

Activity: Watch a video on Bitcoin Nodes

One of the options to run your own node is to download the Bitcoin Core software and give it some time to download the entire blockchain. Once ready, you can leave it on and, approximately every 10 minutes, new blocks with transactions arrive. Your node checks their validity, adding them to your local copy of the blockchain.

Resource: Bitcoin Core Software

Running a node provides sovereignty and independence. You don't rely on others; it's your own traffic cop. Unlike your Bitcoin wallet, which lacks a copy of the blockchain, a node ensures self-sufficiency. Instead of trusting others about your bitcoin holdings (and the state of the Bitcoin network), your wallet communicates with your personal node, making your digital experience more secure and trustworthy.

9.3.2. What Is a Bitcoin Miner and How Does Mining Work?

> The purpose of mining is not the creation of new bitcoin; that’s the incentive system. Mining is the mechanism by which Bitcoin’s security is decentralized.
>
> **Andreas M. Antonopoulos**

An Introduction to the Technical Side of Bitcoin

Miners collect unconfirmed transactions, form a block, and expend energy to look for a valuable key that will **add and secure the block's spot in the blockchain.**

Miners are in a race to add the next block to the blockchain. The sought-after prize is a "valid block hash," cleverly hidden among billions of others, and only a specific key assigned by the network can unlock it.

Picture a massive haystack filled with millions of keys, each representing a unique block hash. The network has chosen one specific key to unlock a valuable reward. Miners rummage through the haystack, testing each key in the lock, but only one lucky miner will discover the perfect match.

Once a miner finds the correct block hash, they share it with the network, along with their created block of new transactions. Other miners verify the solution to make sure it's the right fit. If everything checks out, the block is added to the blockchain, creating a secure and public ledger.

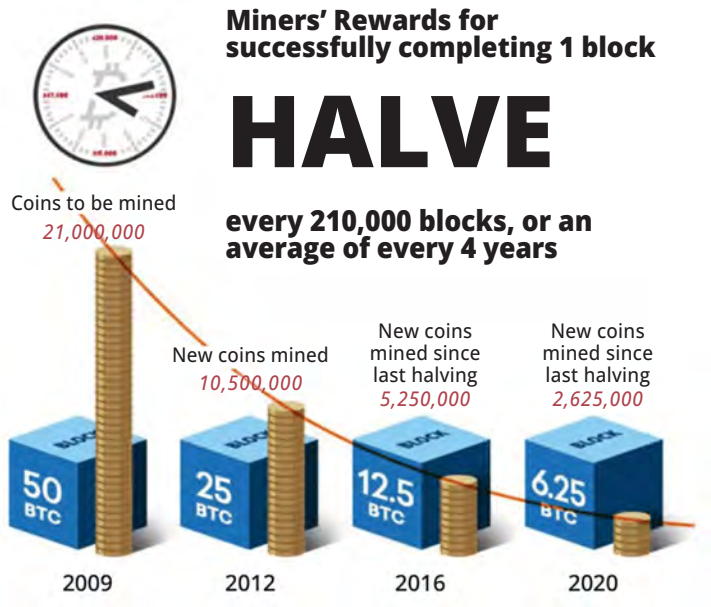
Miners earn rewards for their efforts in two ways: 1 Block rewards 2 Transaction fees

Block rewards are new bitcoins released into circulation with each block added to the blockchain. Transaction fees are small bitcoin payments users make to have their transactions processed faster and prioritized by the miner. Miners can pick which transactions to include in the block they mine, usually giving preference to those with higher transaction fees.

Bitcoin Halvings

A bitcoin halving is an essential part of the Bitcoin universe that helps maintain its scarcity and value over time. As you know, there is a fixed supply of 21,000,000 bitcoins in total. This supply wasn't fully available from the day Bitcoin launched. Instead, this supply enters the Bitcoin universe in a step-by-step fashion.

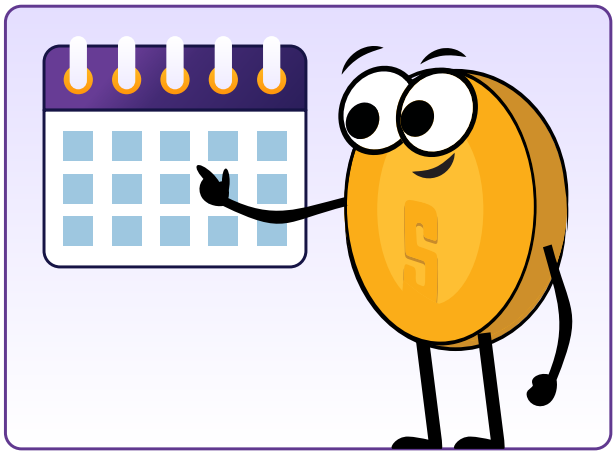
Satoshi Nakamoto cleverly designed a block reward system to distribute new bitcoins without a central authority. In Bitcoin's early days, miners got a sweet 50 bitcoin reward for each block they mined, motivating them to invest in powerful equipment and electricity for their mining operations.



To keep the network stable and manage new bitcoin supply, the block reward is halved about every 210,000 blocks. This event, called "the halving," decreases the number of new bitcoins entering circulation and continues to motivate miners to protect the network and uphold its decentralization. Historically, halving events have led to significant price increases in the Bitcoin market due to the reduced supply of new bitcoins making their way into circulation.

Circulating supply refers to the total amount of a currency. With Bitcoin, the total circulating supply is the number of coins that have been mined and are in circulation at any given time, excluding any coins that are lost forever.

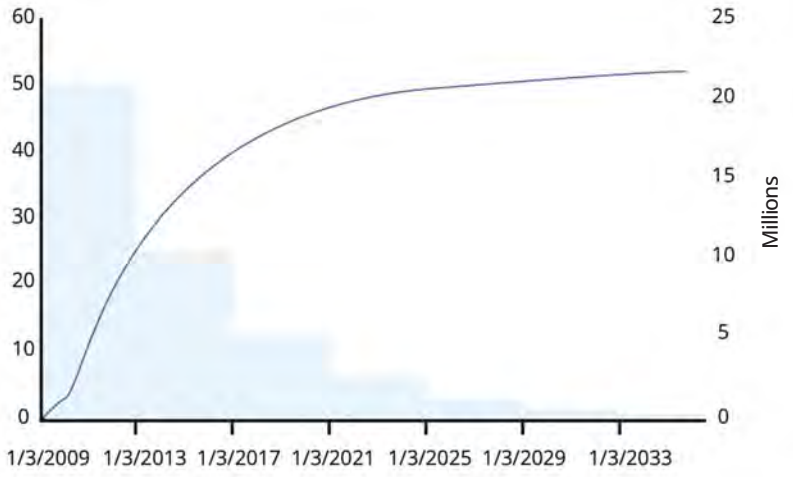
During each halving event, miners receive smaller bitcoin rewards, which lowers the issuance rate of new coins. As a result, Bitcoin's mining difficulty increases to maintain a block time of approximately 10 minutes, ensuring new blocks are added to the blockchain at a steady pace. The reduction in mining rewards doesn't necessarily mean miners make less profit, as they can also earn transaction fees for verifying transactions and adding them to the blockchain, which can offset the decrease in mining rewards.



Halving events are pre-programmed into the Bitcoin protocol, making the supply schedule of bitcoins predictable and transparent.

The **Bitcoin supply schedule** is the predetermined and public plan for the release of new bitcoins into circulation, designed to maintain Bitcoin's scarcity over time.

Bitcoin Supply Schedule



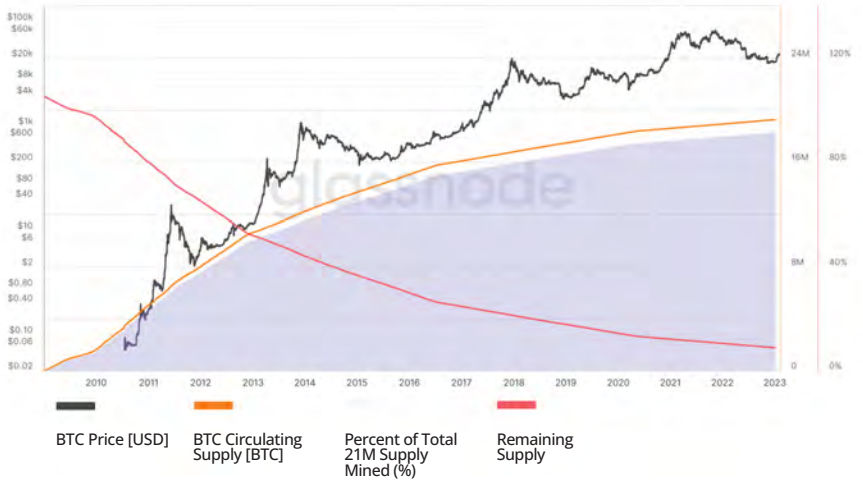
The following table outlines the details of upcoming halving events for Bitcoin, including the expected date of the next halving event, the block number at which the halving event will happen, the block rewards (per mined block) during that halving event, and the percentage of the total supply that will be mined.

Event	Expected Date	Block	Block Reward	Percentage Mined
Fourth Halving	2024	840,000	3.125	96.875 %
Fifth Halving	2028	1,050,000	1.5625	98.4375 %
Sixth Halving	2032	1,260,000	0.78125	99.21875 %

An Introduction to the Technical Side of Bitcoin

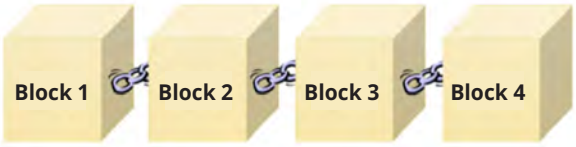
As more bitcoins are mined, the circulating supply and the percentage of the total supply that has been mined will keep increasing until the total supply of 21,000,000 is reached. The reduced supply, combined with rising demand, can boost Bitcoin's price (relative to the dollars). This benefits early adopters and also motivates miners to continue securing the network and contributing their computing power and resources.

Bitcoin: Percent of 21M Supply Mined

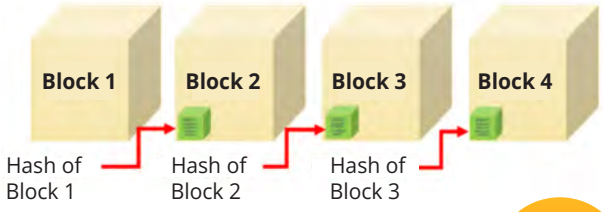


What Is a Valid Block Hash in Bitcoin?

In Bitcoin, a valid block hash is like a special code that miners try to find. It's a unique number that helps keep track of each block in the blockchain that stores information about transactions. The blocks connect in a chain from the first one (genesis block) to the latest, making a public record of all transactions. This block hash is crucial because it links each block to the one before it, making it easy for anyone to check the history of transactions. It's a bit like a fingerprint for each block, ensuring the information is correct and secure. The block hash acts as a way to confirm that the data in the block hasn't been changed.



The blocks are "linked" together by enforcing a specific relationship between blocks. That is, a block must contain a "fingerprint", which is a hash value of the dadata of the previous block. A hash function can condense arbitrary message (the block information) to a fixed size (e.g., 160 bits) and produces a fingerprint of the message.

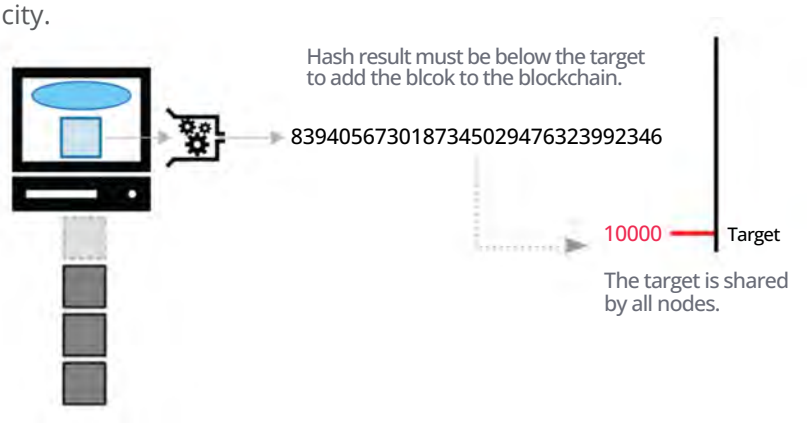


Satoshi Nakamoto, the creator of Bitcoin, mined the initial block, which held a total of 50 bitcoins.

The Race to Mine a Block

Miners engage in a competition to uncover the block hash that aligns with the target (a special number) set by the network. The miner who's the first to successfully discover the correct block hash is granted the opportunity to add that block to the blockchain and assign it with the corresponding hash ID. This solution serves as validation for the block's authenticity.

Mining can be compared to a race where the goal is to reach the finish line as quickly as possible. How difficult it is to find the block hash is adjusted periodically, ensuring that each block continues to be mined in approximately 10 minutes (as miners join and leave). This mechanism is called the "difficulty adjustment."



Let's say the target number set by the Bitcoin network is 1,000. The miners would have to use their computational power and energy to search for a block hash (a specific number) that is lower than 1,000. The first miner to find a block hash lower than 1,000 gets to add the new block to the blockchain and is rewarded with bitcoins.

The difficulty level in Bitcoin mining is a measure of how difficult it is to find a valid block hash that meets the target set by the network. It is adjusted every 2016 blocks, or roughly every two weeks, to ensure that blocks are added to the blockchain at a consistent rate. The difficulty level is expressed as a number, and the higher the difficulty level, the more difficult it is to find a valid block hash.

For example, consider two different hashes:

- **Hash 1:** 0000A1mINgF0RbL0cK5wItHth3hAy5tAcK
  Difficulty level: 1
- **Hash 2:** 00000000A1mINgF0RbL0cK5wItHth3hAy5tAcK
  Difficulty level: 2

In this example, Hash 2 has a higher difficulty level than Hash 1 because it is a longer hash with more zeros at the beginning. It would be harder for miners to find Hash 2 because their computers would need to do more work.

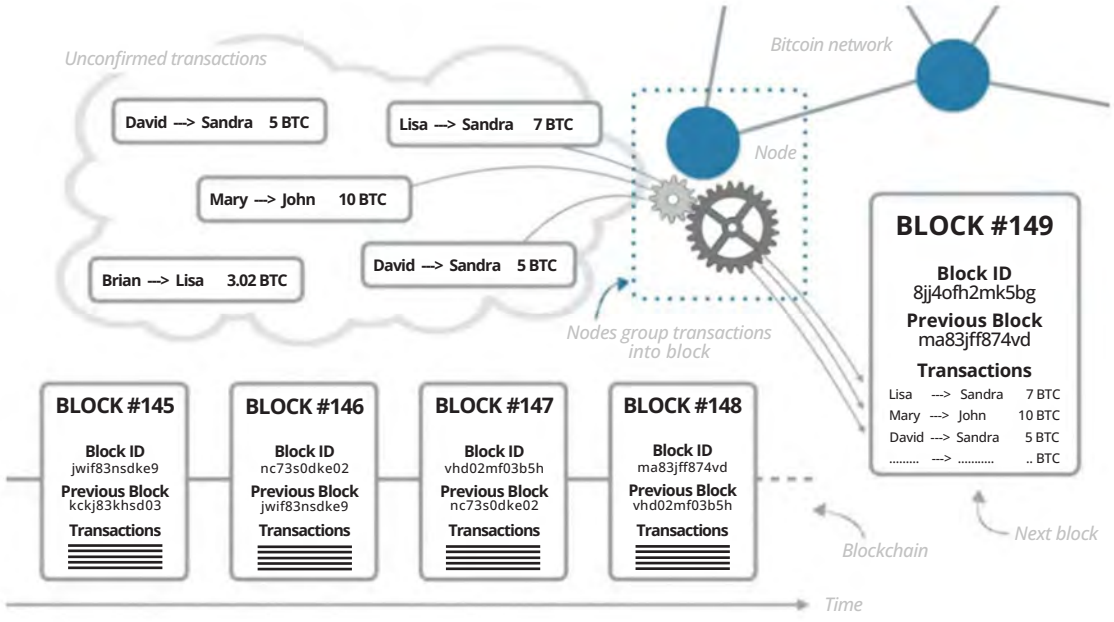
By finding a valid block hash, a miner demonstrates that they have done the work required to add the new block to the blockchain and they are paid a reward in bitcoins, plus transaction fees, for their effort. Proof-of-Work (PoW) is the method the Bitcoin network uses to validate transactions and add new blocks to the blockchain.

An Introduction to the Technical Side of Bitcoin

PoW keeps Bitcoin safe by making it difficult for anyone with malicious intentions to take control.

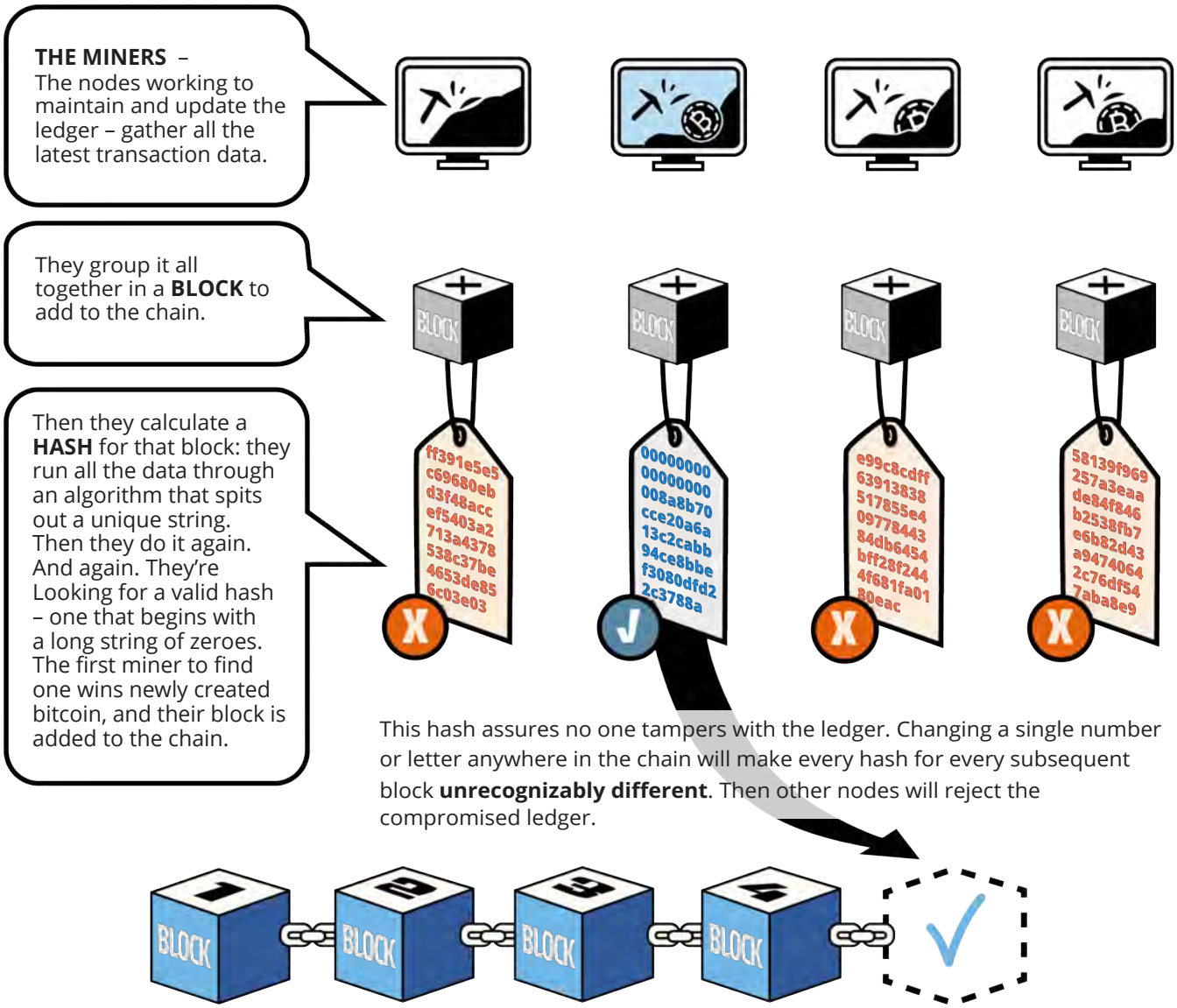
In summary, the miner's tasks consist of:

1. **Bundling Transactions into Blocks:**
   While nodes verify newly created transactions that are waiting in the "Mempool," miners select a subset of these to include in their candidate block.
2. **Proof-of-Work:**
   Miners race with each other to find the valid block hash.
3. **Broadcast Valid Blocks:**
   After finding the valid blockhash, they propagate the new block to the network.
4. **Earn Rewards:**
   Lastly, they receive newly created bitcoins and transaction fees for successfully adding the block to the blockchain.



Multiple miners can work on creating new blocks simultaneously. The first miner to discover a block hash that meets the target set by the network announces it to the network, and the other miners then check the transactions in that miner's candidate block to make sure they are valid. If the transactions are indeed valid, the block is added to the blockchain. The other blocks created by the other miners at the time are not added and are discarded. This process helps maintain consensus within the network and prevents double-spending.

A candidate block is a set of transactions considered for addition to the blockchain that has not been added yet.



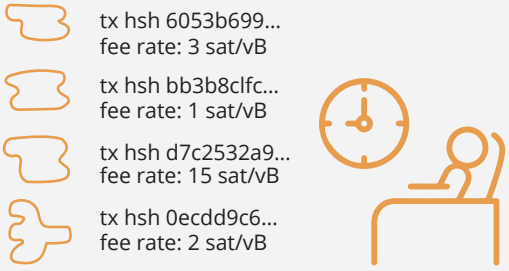
9.4 What Is the Mempool?

The "mempool" or memory pool is like a waiting room for transactions in the Bitcoin network. When you make a transaction, it is first broadcasted to the Mempool before it is verified, selected, and added to the blockchain.

Imagine you are waiting in line at a restaurant. Your name is added to a list of people waiting for a table. When a table becomes available, the host calls your name and seats you. Similarly, a bitcoin transaction is added to the mempool when it is made and is confirmed and added to the blockchain when a miner includes it in a block.

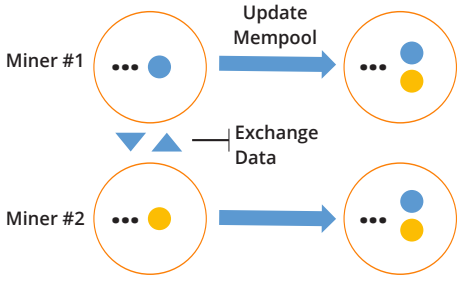
An Introduction to the Technical Side of Bitcoin

A **mempool** is where transactions wait to be confirmed into a block.



When a node first receives a transaction from a peer, it has to verify the transaction is legit. Nobody wants faulty or deceptive transactions.

Mempool synchronization allows nodes to share their transactions with other nodes by sending a message containing a list of **verified** transactions in the mempool.



The main purpose of a **mempool** is to:

1. Relay unconfirmed transactions.

2. Provide miners transactions to mine.

Accept to Memory Pool (ATMP) involves checking things like:

- Do I already have this transaction?
- Is there a conflict with a different transaction in the mempool?
- Does the ***bitcoin*** in cover the ***bitcoin*** out?
- Do the signatures prove the previous outputs can be spent?
- Are there enough fees?

How Are Transactions Verified and Added to the Mempool?

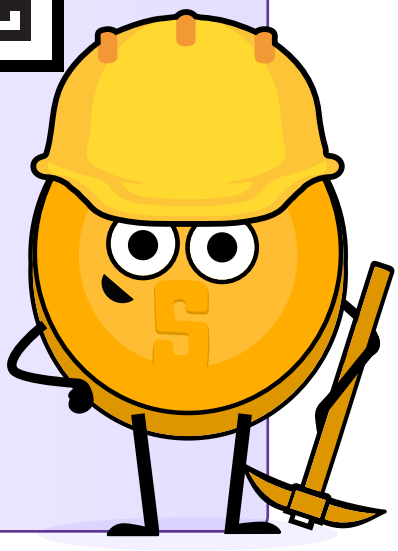
When new transactions are broadcasted to the Bitcoin network, nodes verify these transactions to make sure they are valid and that the funds have not been spent before. Once these transactions are verified, the nodes will add them to their Mempool. The nodes will then share the transactions with other nodes to double-check. Finally, if the majority of nodes agree, the transactions will be made available for miners to select and include them in a block. However, there are several reasons why a transaction might not be confirmed after 72 hours:

1. **Low Transaction Fees:**
   Transactions with low fees may not be processed quickly enough as miners are more likely to choose transactions with higher fees to include in their blocks.
2. **Network Congestion:**
   If the network is congested, there may be a delay in confirming transactions, even if they have a high fee.
3. **Double Spend Attempt:**
   If a malicious actor attempts to double spend, their transaction may be rejected by the network.
4. **Incorrect or Incomplete Data:**
   If a transaction contains incorrect or incomplete data, it may be rejected by the network.
5. **Malformed Transaction:**
   If a transaction is malformed, it may be rejected by the network.

To avoid having transactions rejected, it's recommended to include a fee that is high enough to ensure the transaction is processed in a timely manner and to double — check that all the data in the transaction is correct before sending it.

Activity: Mempool

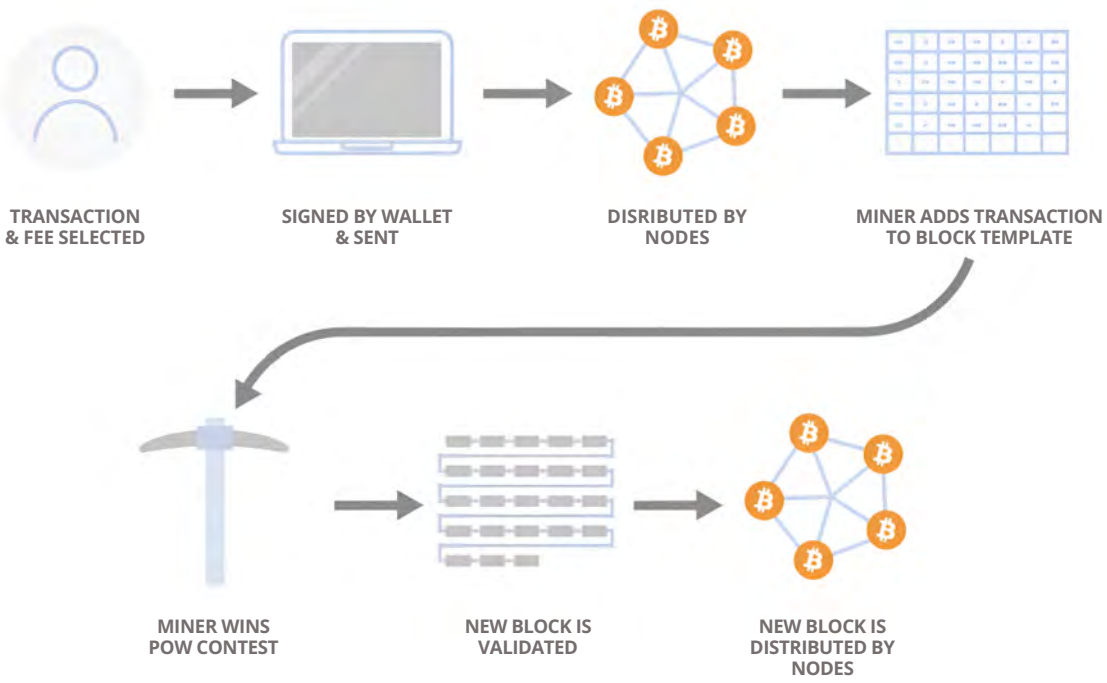
1. Scan the following **QR code:**
2. Review the various elements displayed on the page, including the latest blocks, confirmed transactions, number of transactions, memory usage, and approximate value of the entire block. Answer the questions:
   - What was the last mined block?
   - How many transactions were included in that block?
   - What is the total value traded in bitcoin?
   - What was of the block in megabytes?
   - How many zeros does the nonce of the block start with?How much bitcoins did the miner earn in total?
   - What was the total value of fees received by the miner for adding the transactions to the network?
   - Choose one of the highest-value transactions in the block. How many Bitcoin addresses was the amount distributed to?



An Introduction to the Technical Side of Bitcoin

9.5 How Bitcoin Transactions Work from Start to Finish

1. Adam wants to send bitcoin to Gerardo. He picks one of his UTXOs, creates a transaction, and adds all necessary details, including the amount of bitcoins he wants to send, Gerardo's receiving address, and an above — average transaction fee.
2. After a final check to ensure all details are correct, Adam uses his private key to sign the transaction.
3. Adam broadcasts the transaction to the Bitcoin network.



From: Stevenot, Ted, "What is a bitcoin node and how does one work?". Unchained Capital, 17, January, 2023, https://unchained.com/blog/what-is-a-bitcoin-node/

4. The nodes on the network receive the transaction and verify its validity according to the consensus rules (like checking if Adam's signature is valid and if he has sufficient funds to make the transaction).
5. The transaction is marked valid, and the nodes propagate it to other nodes on the network, adding it to the Mempool.
6. Since Adam picked a high enough transaction fee, almost all miners include his transaction in their blocks.

7. Proof-of-Work: Miners race and try to mine their block by finding the valid block hash. One of the miners finds the hash and broadcasts their block to the network.

8. The nodes receive the newly mined block and verify its validity. This includes validating all transactions within the block and ensuring that the Proof-of-Work requirement is met.

9. The majority of nodes agree that the block is valid and add it to the blockchain. Gerardo receives the confirmed bitcoins at his receiving address.

10. As additional blocks are added to the blockchain in the subsequent hour, the number of confirmations for the transaction grows. As the number of confirmations for the transaction increases, Gerardo gains greater confidence in its success and irreversible nature.

In summary, the sender signs the transaction with their private key, the nodes verify the transaction UTXOs, and the miners add the verified transaction to the blockchain. The receiver can then access the bitcoins using their private key. Once a block is mined, all the transactions included in it are considered confirmed and the UTXOs used as inputs in these transactions are considered spent and will not be used again.

As we wrap up this chapter, you've gained valuable insights into the fundamental concepts of how Bitcoin works. We've covered essential aspects, from the basics of money to the technical side of Bitcoin technology. Now, let's tie it all together in the next chapter. Chapter 10 awaits, where we'll delve into the significant question: "Why Bitcoin?"

Chapter #10

Why Bitcoin?

10.0 Introduction

Activity: What Could a Bitcoin Future Look Like?

10.1 What Are Central Bank Digital Currencies (CBDCs) and Who Controls Them?

10.2 The Philosophy of Bitcoin

Activity: Class Discussion — Do You Have the Right to Control Your Own Money?

10.3 The Benefits of Bitcoin

10.4 An Empowered Future

Activity: Class Discussion — How Did Your Perspective Change?

Student Workbook

English Version | 2025

Why Bitcoin?

10.0 Introduction

> Bitcoin is more than a currency; it's a revolution restoring power to the people, offering a taste of peace and freedom in a world hungry for empowerment.
>
> **My First Bitcoin**

In this concluding chapter, we'll summarize the lessons learned throughout our journey, ask and discuss a few important questions, and explore the future of Bitcoin.

Bitcoin is not just a technology; it's a type of network that powers a new form of money whose supply cannot be changed by any single party. Humanity has never had a form of money with a fixed supply and no centralized control. If widely adopted, Bitcoin is a tool that will unlock a movement for positive change that can transform the lives of people all over the world. It represents a peaceful revolution toward collective freedom and equity, opening up new opportunities for humanity by creating a shared, global monetary system.

As a decentralized global system, Bitcoin enables greater financial freedom, shifting power from the few to the many. It provides a secure, censorship-resistant platform for storing and transferring value, empowering individuals to take control of their wealth and protect their purchasing power. This is especially important in today's uncertain economic climate, where the traditional financial system is facing unprecedented challenges.

Activity: Watch the Video

The possibilities for positive change are immense, which is why we invite you to watch this video to learn more.

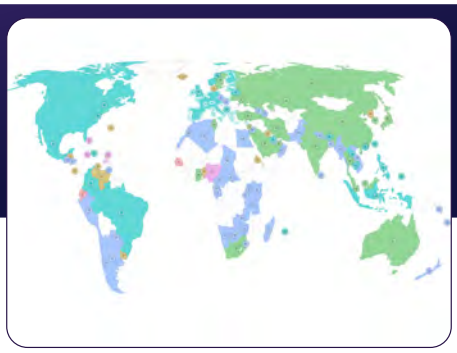
Next, we'll look at another form of digital currency called a Central Bank Digital Currency (CBDC) and evaluate how is similar and different to Bitcoin.

10.1 What are Central Bank Digital Currencies (CBDCs) and Who Controls Them?

Central Bank Digital Currencies, or CBDCs, are digital versions of regular fiat money. CBDCs follow the same rules as regular fiat money, where a central authority, like the government, can create more supply thereby reducing people's purchasing power. However, CBDCs also grant governments new and potent tools to control how that money is used by people around the world.

According to the Human Rights Foundation (HRF) research, 119 out of 193 governments worldwide are looking into, testing, or using CBDCs.

You can check if your country is trying CBDCs on the Human Rights Foundation's CBDC tracker at **https://cbdctracker.hrf.org/home or https://cbdctracker.org/**

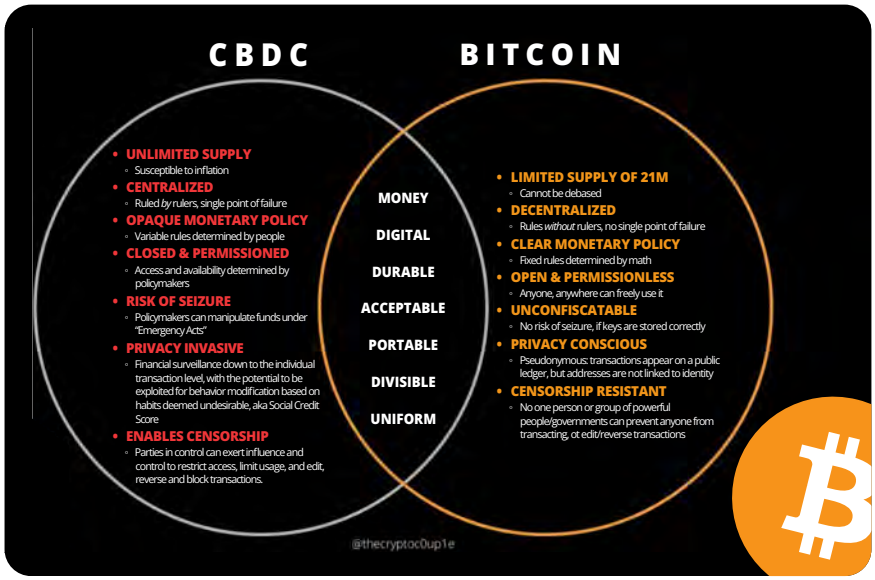


So, what makes CBDCs different from regular fiat money besides being digital? It's crucial to understand that, unlike regular fiat money in the form of paper or coins, CBDCs let the government digitally watch and control every transaction globally. This means the government can stop certain transactions or even freeze your whole account if they don't like you or how you're using your money.

For example, imagine you want to send money to a family member in a country that needs help but your local government rejects your transaction because they don't agree with that country's leaders. Or picture going to the store to buy something you like but you can't because you expressed your opinion on social media.

CBDCs give governments unlimited power to control how money is used around the world, limiting individuals' ability to spend money based on their own choices. Some even argue that CBDCs would enable powerful governments to centrally enforce tyrannical policies on a global scale at the flick of a switch, without the need for human enforcement agents.

Both CBDCs and Bitcoin are digital, but beyond this commonality, they represent very different forms of money with distinct philosophies, leading to varied outcomes for humanity.



10.2 The Philosophy of Bitcoin

In Chapters 6 and 9, we discovered that individuals who run a node help keep Bitcoin's rules safe. This is a big deal because, for the first time ever, people like us can be part of a team that ensures the rules of our monetary system are protected. These rules include the fact that there's only a limited amount of money, and no one single party can change these rules. It's a unique opportunity for regular people to help keep our money secure and reliable.

Bitcoin's philosophy is about empowerment, freedom, financial independence, critical thinking, and the concept that we should all have a say in the rules of the system we choose for ourselves. Unlike the fiat system controlled by powerful central parties, Bitcoin works on a network where no single party has all the control. This means, unlike with other types of money like CBDCs, no one can take your property from you or stop you from spending your money the way you want.

In the fiat world, having more wealth directly translates to having more influence and control. Contrastingly, Bitcoin operates in a way that's all about power to the people. It's a team effort where everyone, no matter how much money they have, plays a crucial role in the system. Imagine it as a collective force, where your financial size doesn't automatically mean you control everything. Bitcoin is built on unchangeable rules, and, in this harmony, it's as if humanity itself is in control of the system. It's not a few big-shots calling the shots; it's all of us working together, as a resilient community, guiding the course of Bitcoin without any single authority telling it what to do.

While in the fiat system the powerful dictate the rules, in the Bitcoin ecosystem, it's the collective strength of individuals that sustains the network. No single entity, regardless of wealth, can dictate the path of the Bitcoin ecosystem. It's an inversion of the traditional power dynamic, where the system's resilience lies not in the hands of the few but in the collective power of every participant.

The main idea is to create a safe, clear, and fair system where everyone can access global money equally.

Activity: Class Discussion — Do You Have the Right to Control Your Own Money?

1. Is money a human necessity and a human right? And why?
2. If you can’t spend your money how you want, send it to who you want, or take your money with you to a new country, is it really yours? And why?
3. Why did barter stop being used? What is the problem with the double coincidence of wants?
4. What historical event was the most impactful for you? Why is it important to understand the Nixon shock and its relevance for everyone today?
5. How is money with a fixed supply different from traditional fiat currencies?

6. When was Bitcoin created, by whom, for what purpose, and how does this purpose define the concept of a decentralized system?
7. What is the difference between a custodial and a non-custodial wallet? What was your favorite wallet?
8. What do you understand about the Lightning Network? What type of transactions would you use it for?
9. Why does running your own node support the network?
10. How does having control over your own money empower you in your daily life and future planning?
11. In what ways can financial freedom enhance your ability to contribute positively to your community or society?

10.3 The Benefits of Bitcoin

”Hyperbitcoinization” is a theoretical future where Bitcoin becomes the dominant global monetary system. This would mean that Bitcoin would be used by everyone, everywhere, and for everything — from buying coffee to paying bills and even buying property.

The growing interest in Bitcoin among individuals, businesses, countries, and governments highlights the potential impact of its widespread adoption on the economy and society. Here are some of the benefits of a hyperbitcoinized world:

1. **A Self-Sovereign Future:**
   A self-sovereign future is one where individuals worldwide have full control over their own digital identity and assets. This could lead to greater financial inclusion, freedom, privacy, and security, and thereby contribute to heightened human flourishing, abundance, and overall happiness.
2. **A Reliable Store of Value:**
   Bitcoin’s digital scarcity makes it a reliable store of value, which could encourage more people to use it as a means of saving for the future.
3. **Changes in Monetary Policy:**
   If Bitcoin were to become widely adopted, it could take away government's ability to control the money supply through traditional monetary policy tools. Mass adoption of Bitcoin would potentially increase people’s purchasing power and encourage society to move toward low-time preference activities.
4. **Enhanced Transparency and Traceability:**
   The tamper-proof and immutable record of all transactions on the blockchain could increase transparency and accountability in various industries and sectors. Currently, powerful entities have the ability to move trillions of dollars around the world without clear visibility into where these funds go or how they are utilized. By providing an open and verifiable record of financial transactions, Bitcoin could ensure that the movement of capital becomes more accountable and accessible to the public.

5

A Revolution in the Remittance Market:

The remittance market involves the transfer of funds from one party to another, often across international borders. Despite declining costs, remittances remain relatively expensive compared to domestic bank transfers, especially for smaller amounts. The Lightning Network offers fast and inexpensive transactions, making it well-suited for the remittance market and addressing the high costs and other challenges associated with remittances, such as slow settlement times and restrictions on business hours.

6

Abundant Energy:

When there's a lot of affordable energy, societies do well, and many industries and communities can meet the increasing need for power in homes, businesses, and new technologies. Bitcoin mining incentivizes miners to use surplus energy that would usually go to waste from sustainable energy sources like solar, wind, and hydroelectric power. Bitcoin miners use this surplus energy to create new bitcoins through mining activities, secure the network, and offer excess energy they create back to the energy grid society uses when it is needed.

10.4 An Empowered Future

Bitcoin is money.

Money helps people communicate which activities, goods, and services are most important within society. As we have seen in this course, when money is controlled by centralized authorities, it will be manipulated.

One of the mistakes humanity keeps repeating throughout history is manipulating money, which then negatively affects individuals, families, businesses, governments, and ultimately global human prosperity.

By taking control of money out of the hands of centralized parties and instead using money with a fixed supply that no single party can change, we create a different world — one where we don't have to trust that people will do the right thing but rather one in which people is unable to do the wrong thing.

This is a fundamentally different world.

And you, dear student, can be a part of creating this world. By using Bitcoin, running your own node, and helping your fellow humans learn more about the future of money, you are voting for a different world.

Activity: Final Class Discussion — How Did Your Perspective Change?

Please answer the five questions below:

Why do we need money?

What is money?

Why Bitcoin?

Who controls money?

What gives money its "value"?

Write down the questions posed by students that were selected during Chapter 1 and answer them.

1. **Go back to the first activity in Chapter 1 and compare your new answers to your old answers.**
2. **Compare and discuss the original answers and questions. Did something change?**
3. **Ask yourself this final question: What is my next step? And how can I use this new knowledge to empower myself?**

If you're ready to take the next step, check out the additional resources in the following section, where we have selected the best resources for further learning and success.

Additional Resources

1. Why Use Bitcoin?

a **"The Bullish Case for Bitcoin" by Vijay Boyapati:**

This article makes the case for why Bitcoin is a valuable asset and why it has the potential to become a dominant global currency. The author covers the technical and economic aspects of Bitcoin that make it a strong investment opportunity.

b **"Why Bitcoin Matters" by Aleks Svetski (1 hour):**

This video covers the importance of Bitcoin as a decentralized digital asset and how it can impact the current financial system. The speaker explores the potential for Bitcoin to bring financial freedom to people around the world.

c **"Why Bitcoin" by Wiz:**

This article provides an overview of the benefits of using Bitcoin as a currency and store of value. It highlights the decentralized nature of Bitcoin and how it allows for greater financial freedom and security.

2. What Is Bitcoin?

a **"How Bitcoin Works under the Hood" by CuriousInventor:**

https://www.youtube.com/watch?v=Lx9zgZCMqXE This video provides a detailed explanation of the technical aspects of Bitcoin and how it works.

b **"What Is Bitcoin" by Greg Walker:**

This article provides a comprehensive explanation of what bitcoin is, including its history, technology, and how it differs from traditional currencies.

c **"Bitcoin - The Genesis" by RT (30 minutes):**

This video covers the creation and early days of Bitcoin. It explores the motivations of the mysterious creator, Satoshi Nakamoto, and how the concept of Bitcoin evolved.

3. Further Learning:

a **"The Bitcoin Standard" (1 hour 40 minutes):**

This audiobook explores the economic and historical context that led to the creation of Bitcoin. It covers the benefits of a decentralized currency and the potential for Bitcoin to become a global standard.

b **"Intro to Bitcoin Austrian Thought" (1 hour):**

This audio lecture covers the Austrian School of economics and how it relates to the concept of Bitcoin. It provides an in-depth look at the economic principles behind Bitcoin and how it aligns with Austrian thought.

c **"Bitcoin Babies"**

by Naomi Wambui - **https://bitcoinbabies.com/**
Twitter: **@btcbabies - @ngachanaomi1**
A free PDF resource that aims to empower mothers with essential knowledge encompassing nutrition, Bitcoin, and overall mental well-being.

d **BTC Sessions**

A Bitcoin-only education YouTube channel with useful tutorials and guides:
https://www.youtube.com/@BTCSessions

4. Courses:

a **Summer of Bitcoin**

https://www.summerofbitcoin.org/: A global, online summer internship program focused on introducing university students to Bitcoin open-source development and design.

b Chaincode Labs

https://learning.chaincode.com/#FOSS: Online courses and a residency program which enables students to learn the skills necessary to work on Bitcoin protocol development.

c Saylor Academy

Free education across multiple disciplines: **https://www.saylor.org/**

5. Important Authors

a. Alex Gladstein: *Check Your Financial Privilege*

b. Alex Swan: *Grounded-Encounter Therapy: Perspectives, Characteristics, and Applications*

c. Amanda Cavaleri: *Bitcoin and the American Dream: The New Monetary Technology Transcending Our Political Divide*

d. Anita Posch: *Learn Bitcoin: Become Financially Sovereign*

e. Eric Yakes: *The 7th Property: Bitcoin and the Monetary Revolution*

f. Jeff Booth: *The Price of Tomorrow: Why Deflation is the Key to an Abundant Future*

g. Jimmy Song: *The Little Bitcoin Book: Why Bitcoin Matters for Your Freedom, Finances, and Future*

h. Nik Bhatia: *Layered Money: From Gold and Dollars to Bitcoin and Central Bank Digital Currencies*

i. Robert Breedlove: *Thank God for Bitcoin: The Creation, Corruption, and Redemption of Money*

j. Lyn Alden: *Broken Money*

6. Cited Authors

a Curious Inventor:

https://www.youtube.com/@CuriousInventor

b Anil Patel:

Twitter: @anilsaidso

7. Other Resources:

1. **Bitcoin.org:** The official website of the Bitcoin protocol.
2. **Bitcointalk.org:** Bitcointalk is a forum where users can discuss Bitcoin-related topics, ask questions, and share information. It's a great place to learn from other Bitcoin enthusiasts and experts.
3. **Bitcoincore.org:** This is the original Bitcoin software and is still widely used by many users and developers. It provides a powerful set of tools for interacting with the Bitcoin network and building Bitcoin applications.
4. **Bitcoinwiki.org:** This is a community-driven resource that provides a comprehensive guide to everything related to Bitcoin. It covers everything, from the technical aspects of Bitcoin to its history and use cases.
5. **Bitcoinmagazine.com:** This is an online publication that covers news and insights related to Bitcoin and other cryptocurrencies. It provides a great way to stay up-to-date with the latest developments in the Bitcoin ecosystem.
6. **Bitcoin.Design:** An open-source repository of bitcoin-related design files for illustrations, websites, templates, and icons.
14. **Yzer:** https://yzer.io/ Simple, mobile, Bitcoin education. Learn about Bitcoin, finance, economics, and earn Sats.
7. **NOSTR:** https://nostr.com/ - Social media where you actually own your data.
8. **Simple X:** https://simplex.chat/ - A private, decentralized application protocol.
9. **Set up a Bitcoin Node:** Raspberry Pi DIY by Keith Mukai: https://github.com/kdmukai/raspi4_bitcoin_node_tutorial?tab=readme-ov-file
10. **How to select a Bitcoin wallet:** https://bitcoin.org/en/choose-your-wallet - Use your newly gained knowledge to select the right wallet for you.
11. **BitcoinIcons.com:** - https://bitcoinicons.com/ - A collection of free Bitcoin icons.
12. **Bitcoin For Local Business:** https://bitcoinforlocalbusiness.com/ - A set of fliers to help you share the value of Bitcoin with your favorite local businesses.
13. **Mempool.Space:** https://mempool.space/ - An open source Mempool project which also features Lightning Network data and graphs.

Chapter Key Concepts

Chapter 1:

Course Introduction:

Explore the course objectives and expectations for the Bitcoin Diploma.

Reflective Activity — Defining Money:

Engage in a reflective exercise by providing five answers to key questions about money.

Class Discussion — Why We Need Money:

- Participate in a class-wide discussion exploring the fundamental necessity of money.
- Share and compare individual perspectives on the importance of money.
- Lay the groundwork for understanding the role of money in economic systems.

Chapter 2:

Understanding Money:

- Explore the fundamental definition and concept of money.
- Discuss the diverse perspectives within the class to grasp the multifaceted nature of money.

Functions, Properties, and Types:

- Delve into the functions, properties, and types of money.
- Recognize the importance of these aspects in defining and utilizing money.

Psychology of Money:

- Understand the psychological aspects of money, including scarcity, time preference, and tradeoffs.
- Engage in the "Time Preference" activity to relate psychological elements to real-life scenarios.

Chapter 3:

Introduction to Money's History and Evolution:

Explore the history and evolution of money. Understand how ancient forms of trade led to the development of the currency we use today.

Digital Currency Revolution:

- Discover the current pinnacle of money's evolution — digital currency.
- Understand how it exists only in electronic form, enabling instantaneous, low-cost transactions globally.
- Learn about the significant role Bitcoin played in solving early challenges of digital currencies, making them ready for worldwide use.

Evolution of Currency:

Explore the transition from ancient forms like shells and beads to the emergence of coinage and paper money. Follow the journey from paper to plastic, unraveling the evolution of currency throughout history.

Barter Game Activity:

Engage in a hands-on barter game experience to grasp the challenges of direct exchange and appreciate the need for a more efficient system.

Chapter 4:

Fiat Money Origins:

Explore the origins of fiat money through a brief historical overview, understanding how it became a dominant form of currency.

Fractional Reserve Banking Activity:

Engage in the Fractional Reserve Banking activity to gain insights into how this system operates, highlighting its reliance on debt and the implications for the broader economy.

The Fiat System:

Grasp the fundamental aspects of the fiat system, including its nature as a monetary system by decree, the role of fractional reserve banking, and the key players controlling this system.

Chapter 5:

Decreasing Purchasing Power:

Understand the concept of monetary inflation and its impact on purchasing power. Engage in the Effects of Inflation: An Auction Activity to experience the effects firsthand.

The Fiat System's Consequences Activity:

Participate in the Consequences of the Fiat System activity, shedding light on the broader repercussions of the current monetary framework.

Central Bank Digital Currencies (CBDCs):

Explore the evolving landscape of Central Bank Digital Currencies (CBDCs) and their potential impact on the future of money.

Global Debt Burden and Social Inequality:

Explore the dual impacts of the global debt burden and social inequality. Recognize the individual and societal consequences, emphasizing the loss of purchasing power and the widening wealth gap.

The Cypherpunks and Decentralization:

Learn the Cypherpunks' story and their motivation for seeking a decentralized currency. Differentiate between centralized and decentralized systems, gaining insights from a brief history of digital currencies.

Chapter 6:

Satoshi Nakamoto and Bitcoin's Creation:

Explore the mysterious figure of Satoshi Nakamoto and the origin story of Bitcoin, understanding the initial motivations behind its development.

Class Activity — Consensus Building:

Engage in the Consensus Building in a Peer-to-Peer Network activity to gain practical insights into how consensus is achieved within the Bitcoin network.

Embracing Personal Responsibility:

Emphasize the concept of personal responsibility in the context of Bitcoin, encouraging an understanding of individual roles and accountability within the decentralized ecosystem.

How Bitcoin Works:

A look into the mechanics of Bitcoin, including the Nakamoto Consensus Mechanism. Identify the key players in the Bitcoin network, such as miners, nodes, users, developers, and projects, and grasp the collaborative dynamics between them.

Bitcoin as Sound Digital Money:

Examine Bitcoin's role as sound digital money, discussing its evolution, functions, and properties, and participate in a class discussion on whether Bitcoin qualifies as sound money.

Chapter Key Concepts

Chapter 7:

Peer-to-Peer Transactions:

Engage in decentralized transactions to experience the core principles of Bitcoin exchanges.

Setting Up a Bitcoin Wallet:

Learn the essential steps to download, create keys, and back up a Bitcoin wallet for secure transactions.

Saving and DYOR:

Understand saving in Bitcoin as a store of value and the importance of independent research for informed decision-making.

Bitcoin Wallet Types:

Differentiate between open source, closed source, custodial, and noncustodial wallets, understanding the role of keys in security.

Acquiring Bitcoin:

Explore methods like peer-to-peer transactions and exchanges, discussing privacy concerns related to KYC processes.

Chapter 8:

Introduction to Lightning Network:

Recognize the evolution of Bitcoin through technologies like the Lightning Network, enhancing its capabilities.

Setting Up a Lightning Wallet:

Learn the essential steps to set up a Bitcoin Lightning wallet, facilitating faster and more scalable transactions.

Hands-On Activity:

Engage in a practical Lightning wallet relay race, promoting a dynamic understanding of Lightning Network transactions.

Lightning Wallet Types:

Differentiate between open source, closed source, custodial, and noncustodial Lightning wallets for varied user preferences.

Lightning Transactions:

Explore the process of sending and receiving Lightning transactions, emphasizing the speed and efficiency of the Lightning Network.

Chapter 9:

The Bitcoin Ledger:

Understand the concept of a decentralized ledger facilitated by nodes and miners, ensuring transparency and security.

The UTXO Model:

Grasp the Unspent Transaction Output model as a fundamental aspect of Bitcoin's transaction process.

Public and Private Keys:

Explore the significance of cryptographic security in Bitcoin transactions through public and private keys, along with an activity demonstrating SHA 256 hashing.

Bitcoin Nodes and Miners:

Look into the roles of nodes and miners in maintaining the Bitcoin network, covering aspects like issuance, scarcity, halving, and difficulty.

How Bitcoin Transactions Work:

Gain insight into the entire lifecycle of a Bitcoin transaction, involving the sender, receiver, nodes, miners, and the mempool, with a dedicated activity focused on the mempool.

Chapter 10:

Philosophical Underpinnings of Bitcoin:

Explore the foundational philosophy behind Bitcoin, understanding how it emerged as a response to economic challenges, with a focus on its impact on financial freedom and how it differs from traditional currencies.

Bitcoin's Future:

Delve into the potential trajectory and future developments of Bitcoin as a revolutionary digital currency.

Diploma Reflection:

- Summarize key takeaways from the Bitcoin Diploma, encouraging students to reflect on their journey and insights gained.
- Activities include watching a video on "why Bitcoin?" and revisiting Chapter 1's questions to assess personal growth in understanding.

Glossary

51% Attack: A type of attack on a blockchain network in which a single entity or group controls a majority of the network's computing power, allowing them to manipulate transactions and potentially disrupt the network.

Altcoin Season: A period of time when alternative cryptocurrencies experience significant price increases, often due to increased investor interest and adoption.

Altcoins: Digital currencies excluding Bitcoin.

Atomic Swap: A peer-to-peer exchange of one cryptocurrency for another without the need for a centralized exchange or intermediary.

Auction: A process by which goods or assets are sold to the highest bidder.

Bartering: The exchange of goods and services without the use of money.

Basket of Goods: A collection of goods or services used to measure changes in the cost of living.

Bitcoin: A digital currency/system that allows people to send money to each other without using a bank.

Block Explorer: A tool used to view and explore the blockchain, allowing users to view individual blocks, transactions, and wallet addresses.

Block Reward: The amount of new bitcoins that are awarded to miners for adding a new block to the blockchain.

Blockchain: A public record of all bitcoin transactions that have taken place.

BTC: The unit used for bitcoins. A digital currency that can be used to make purchases or be traded.

Capital Controls: Restrictions on the movement of money across borders.

Central Bank (Fed): A government-owned institution that manages a country's monetary policy.

Centralization: The concentration of power or control in a single entity.

Centralized System: A system in which power or control is concentrated in a single entity.

Cold Storage: A method of storing bitcoins offline, away from the risk of hackers or other online threats.

Commodity Money: Objects that have value in and of themselves and are used as a medium of exchange, such as gold or silver.

Confirmation: The process of a transaction being processed by the network and highly unlikely to be reversed. The method by which "miners" verify the authenticity of transactions with their computer hardware and software. It is recommended to wait for at least six confirmations to prevent double spending.

Consensus Mechanism: A method used in blockchain technology to validate transactions and ensure the integrity of the blockchain.

Cryptocurrency Exchange: A platform where users can buy, sell, and trade cryptocurrencies for other assets such as fiat currency or other cryptocurrencies.

Cryptocurrency Wallet: A software program that stores private keys and allows users to send, receive, and manage their cryptocurrency.

Cryptography: A branch of mathematics that helps create secure systems.

Debasement: The reduction in the value of a currency, often by reducing the amount of precious metal in a coin.

Debt: Money that is owed to someone else.

Decentralization: The distribution of power and control across a network rather than having a central authority.

Decentralized Autonomous Organization (DAO): An organization or network governed by smart contracts and run on a blockchain without a central authority or management structure.

Decentralized Finance (DeFi): A movement within the cryptocurrency industry to create decentralized financial products and services that operate on a blockchain.

Decentralized System: A system in which power or control is distributed among multiple entities.

Digital Asset: A digital representation of value that can be traded or used as a store of value, such as bitcoins.

Distributed Ledger: A database that is spread across a network of computers rather than being stored in a central location.

Double Coincidence of Wants: The phenomenon where two parties in a barter economy both have what the other party wants and wants what the other party has.

Double Spend: When a person tries to send their bitcoins to two different recipients at the same time.

Dust Transaction: A transaction that sends a very small amount of bitcoins that is too small to be economically viable.

Glossary

Exchange Rate: The value of one currency in relation to another.

FOMO: Fear of missing out, a term used to describe the feeling of anxiety or regret that one may miss out on a profitable opportunity in the cryptocurrency market.

FUD: Fear, uncertainty, and doubt, a term used to describe negative rumors or information that can cause market panic or decline.

GDP: Gross domestic product, the total value of goods and services produced in a country in a given period of time.

Hard Fork: A change to the Bitcoin protocol that creates a new version of the blockchain that is not compatible with the previous version (i.e. Bitcoin Cash).

Hardware Wallet: A physical device used for storing private keys and managing cryptocurrency, providing enhanced security over software wallets.

Hash Function: A mathematical function that takes input data of any size and outputs a fixed-size string of characters, commonly used in cryptography and blockchain technology.

Hash Rate: A way to measure the processing power of the Bitcoin network.

HODL: A term used in the cryptocurrency community to describe holding onto cryptocurrency long-term rather than selling or trading it.

Hot Wallet: A Bitcoin wallet that is connected to the internet, allowing for easy access to bitcoins.

Imports: Goods and services produced in another country and sold in the domestic market.

Inflation: An increase in the general price level of goods and services in an economy.

Initial Coin Offering (ICO): A fundraising method in which a new cryptocurrency is sold to investors in exchange for a more established cryptocurrency, such as Bitcoin.

Layer-1 Protocol: The underlying layer of a blockchain network that handles the fundamental aspects of consensus, transaction validation, and data storage.

Layer-2 Protocol: A secondary layer built on top of a layer-1 blockchain network, often used to enhance scalability, speed, and functionality.

Ledger: A record of financial transactions.

Lightning Network: A layer-2 payment protocol that enables faster and cheaper bitcoin transactions by using off-chain channels for smaller transactions.

Mediums of Exchange: Objects or systems that are widely accepted in exchange for goods and services.

Merkle Tree: A tree-like data structure used in the Bitcoin blockchain to efficiently verify the integrity of large sets of data.

Mining Pool: A group of miners who work together to increase their chances of finding new blocks and earning bitcoins.

Mining: The process of using computer hardware to do mathematical calculations for the Bitcoin network to confirm transactions and increase security.

Monetary and Fiscal Policy: The policies of a central bank and government, respectively, that influence the money supply and interest rates in an economy.

Money Supply: The total amount of money in circulation in an economy.

Multi-Signature (Multisig) Wallet: A wallet that requires multiple signatures or approvals before a transaction can be executed, providing additional security and control.

Multi-Signature: A security feature that requires more than one private key to authorize a bitcoin transaction.

Network: A group of interconnected entities.

Node Network: A network of connected computers or devices that support and maintain the Bitcoin network.

Node: A computer or device that is connected to the Bitcoin network and participates in the verification and transmission of transactions.

Non-Fungible Token (NFT): A type of digital asset that represents a unique or one-of-a-kind item, often used to represent art, collectibles, or other unique objects.

Nonce: A random number added to a block header to create a hash that meets the difficulty target.

Orphan Block: A block not included in the main chain of the blockchain due to being invalidated by a longer competing chain.

Paper Wallet: A printed copy of a user's private and public keys used for storing and managing cryptocurrency offline.

Peer-to-Peer (P2P): A decentralized network in which participants interact directly with each other rather than through a central authority.

Glossary

Peg: A fixed exchange rate between two currencies where one is pegged to the value of another.

Private Blockchain: A blockchain controlled by a single organization rather than being decentralized.

Private Key: A secret piece of data that proves a person's right to spend bitcoin from a specific wallet through a cryptographic signature.

Proof-of-Stake (PoS): A consensus mechanism used in some blockchain networks that requires users to hold a certain amount of cryptocurrency to participate in the validation of transactions.

Proof-of-Work: A consensus mechanism that requires users to perform a certain amount of computational work to participate in the network.

Public Blockchain: A blockchain open to anyone to participate in and verify transactions, making it decentralized.

Public Key: A unique identifier used for receiving bitcoins derived from a user's private key through a mathematical process.

Public Key/Bitcoin Address: A public password/number used to receive bitcoins.

Public Ledger: A decentralized database that keeps a public record of all transactions on the Bitcoin network.

Purchasing Power: Money's ability to buy goods and services.

Recovery Phrase/Seed Keyword: A series of 12, 18, or 24 words that can be used to generate multiple pairs of private and public keys. These can be used to restore a Bitcoin wallet.

Reserve Ratio: The proportion of deposits that a bank must hold as reserves.

Restrictive Banking: Restrictions or limitations on banking services or access to banking services.

Satoshi Nakamoto: The pseudonym used by the anonymous creator(s) of Bitcoin.

Satoshi: The smallest unit of Bitcoin, equal to 1/100,000,000 of a bitcoin. It is named after the creator of Bitcoin, Satoshi Nakamoto.

Satoshis per Byte (sat/b): A unit used to measure the bitcoin transaction fee paid per byte of transaction data.

SegWit (Segregated Witness): A Bitcoin protocol upgrade that changes the way data is stored on the blockchain, allowing for increased capacity and lower transaction fees.

Sidechain: A blockchain connected to another blockchain, allowing for the transfer of assets or information between the two chains.

Signature: A mathematical mechanism that allows someone to prove ownership.

Smart Contract: A self-executing contract with the terms of the agreement written into code.

Soft Fork: A change to the Bitcoin protocol that is backward-compatible with older versions of the software.

Stablecoin: A type of cryptocurrency designed to maintain a stable value often by being pegged to a fiat currency or other asset.

Supply and Demand: The economic principle that the price of goods or services is determined by the interaction of the quantity of the goods or services supplied and the quantity demanded.

Time Value of Money: The principle that money is worth more in the present than in the future.

Token: A unit of value created on a blockchain often used to represent a specific asset or utility within a particular ecosystem.

Tokenization: The process of creating a digital representation of an asset or asset class on a blockchain, allowing for fractional ownership and transferability.

Trading Pair: A set of two currencies or assets that can be traded against each other on a cryptocurrency exchange.

Transaction Fee: A small amount of bitcoins paid by the sender of a transaction, incentivizing miners to include the transaction in a block and add it to the blockchain.

Transaction ID: A string of numbers and letters that shows the details of a bitcoin transfer (such as the amount sent, the addresses of the sender and recipient, and the date of the transfer) on the Bitcoin blockchain.

Transaction: The transfer of bitcoins from one address to another on the Bitcoin network.

Trustless: A system or transaction that does not require trust in any third party or intermediary. instead relying on the security and transparency of the underlying technology.

Glossary

Two-Factor Authentication (2FA): A security measure that requires two methods of authentication, typically a password and a separate code or device, to access an account or complete a transaction.

Unbanked: Individuals or communities without access to traditional banking services.

Unit of Account: A standard unit of measurement used to express the value of goods and services.

Volatility: The degree of variation in the price of an asset over time.

Wallet Address: A unique identifier used to send and receive bitcoins on the Bitcoin network, typically represented as a string of letters and numbers.

Wallet Backup: A copy of the private keys and recovery phrase/seed keywords of a Bitcoin wallet, which can be used to restore access to the wallet in case the original is lost or stolen.

Wallet: A virtual container for bitcoins similar to a physical wallet that contains private key(s) that allow you to spend the bitcoins allocated to it in the blockchain.

Whale: An individual or organization that holds a significant amount of cryptocurrency, capable of influencing market prices through large trades.

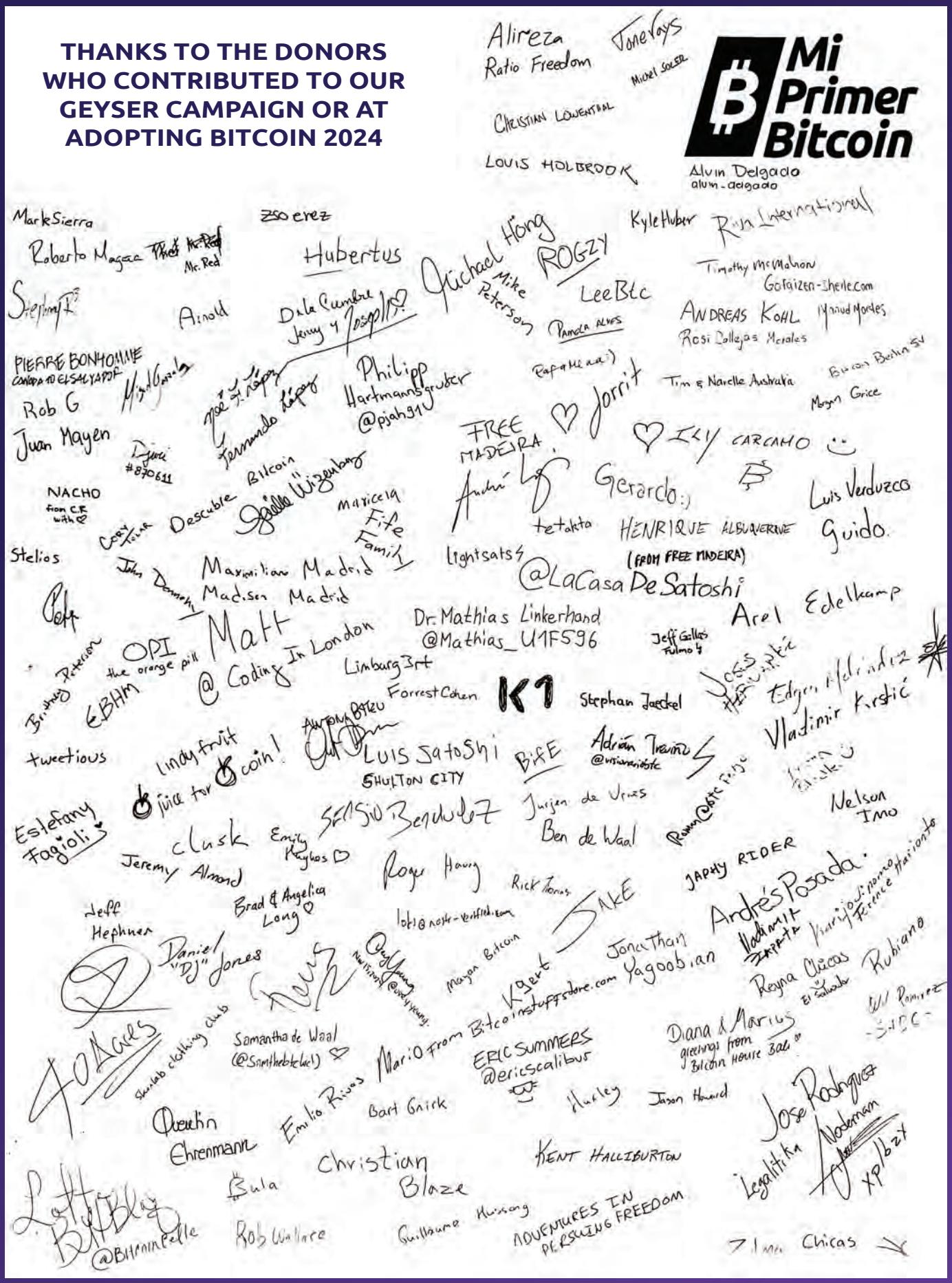
White Hat Hacker: An ethical hacker who uses their skills to identify and fix vulnerabilities in computer systems and networks.

Whitepaper: A report that explains the problem that a blockchain project or cryptocurrency is trying to address and its solution.

XBT and BTC: Abbreviations for bitcoin.

Independent because of you!

THANKS TO THE DONORS WHO CONTRIBUTED TO OUR GEYSER CAMPAIGN OR AT ADOPTING BITCOIN 2024



Thank you!

My First Bitcoin

EL SALVADOR

English Version | 2025